SOPHOS
Security made simple.

SOPHOS
IPS Signature Update
Release Notes

Version : 9.17.79
Release Date : 19th January 2020

Release Information

Upgrade Applicable on

IPS Signature Release	Version 9.17.78
Sophos Appliance Models	CR250i, CR300i, CR500i-4P, CR500i-6P, CR500i-8P, CR500ia, CR500ia-RP, CR500ia1F, CR500ia10F, CR750ia, CR750ia1F, CR750ia10F, CR1000i-11P, CR1000i-12P, CR1000ia, CR1000ia10F, CR1500i-11P, CR1500i-12P, CR1500ia, CR1500ia10F CR25iNG, CR25iNG-6P, CR35iNG, CR50iNG, CR100iNG, CR200iNG/XP, CR300iNG/XP, CR500iNG-XP, CR750iNG-XP, CR2500iNG, CR25wiNG, CR25wiNG-6P, CR35wiNG, CRiV1C, CRiV2C, CRiV4C, CRiV8C, CRiV12C, XG85 to XG450, SG105 to SG650

Upgrade Information

Upgrade type: Automatic

Compatibility Annotations: None

Introduction

The Release Note document for IPS Signature Database Version 9.17.79 includes support for the new signatures. The following sections describe the release in detail.

New IPS Signatures

The Sophos Intrusion Prevention System shields the network from known attacks by matching the network traffic against the signatures in the IPS Signature Database. These signatures are developed to significantly increase detection performance and reduce the false alarms.

Report false positives at support@sophos.com, along with the application details.

This IPS Release includes Two Thousand, Seven Hundred and Sixty Two(2762) signatures to address One Thousand, Nine Hundred and Thirty Eight(1938) vulnerabilities.

New signatures are added for the following vulnerabilities:

Name	CVE–ID	Category	Severity
		Malware Communication	4
	CVE-2017-0144	Malware Communication	2
BROWSER-CHROME Google Chrome CVE-2020-6388 AudioArray Memory Corruption	CVE-2020-6388	Browsers	2
BROWSER-CHROME Google Chrome FileReader CVE-2019-5786 Use After Free (Published Exploit)	CVE-2019-5786	Browsers	2
BROWSER-CHROME Google Chrome FileReader CVE-2019-5786 Use After Free	CVE-2019-5786	Browsers	1
BROWSER-CHROME Google Chrome Integer Overflow Vulnerability	CVE-2019-5789	Browsers	1
BROWSER-CHROME Google Chrome Object Corruption Vulnerability	CVE-2018-6106	Browsers	1
BROWSER-CHROME Google Chrome Out-Of-Bounds Vulnerability	CVE-2017-5053	Browsers	1
BROWSER-CHROME Google Chrome	CVE-2020-	Browsers	1

ReadableStream out of bounds read attempt	6390		
BROWSER-CHROME Google Chrome Use-After-Free Vulnerability	CVE-2019-5788	Browsers	1
BROWSER-CHROME Google Chrome blink webaudio module use after free attempt	CVE-2019-13720	Browsers	1
BROWSER-CHROME Google Chrome desktopMediaPickerController use after free attempt	CVE-2019-13767	Browsers	1
BROWSER-CHROME Google Chromium ImageCapture use after free attempt	CVE-2019-13687	Browsers	1
BROWSER-FIREFOX Apache Tika Chmparser Denial Of Service CVE-2018-1339	CVE-2018-1339	Browsers	2
BROWSER-FIREFOX Mozilla Firefox 3.5 unicode stack overflow attempt	CVE-2009-2479	Browsers	2
BROWSER-FIREFOX Mozilla Firefox Array.prototype.pop type confusion attempt	CVE-2019-11707	Browsers	2
BROWSER-FIREFOX Mozilla Firefox CVE-2017-5428 createImageBitmap	CVE-2017-5428	Browsers	2

Integer Overflow			
BROWSER-FIREFOX Mozilla Firefox CVE-2017-5459 WebGL Integer Overflow I	CVE-2017-5459	Browsers	3
BROWSER-FIREFOX Mozilla Firefox CVE-2017-5459 WebGL Integer Overflow II	CVE-2017-5459	Browsers	3
BROWSER-FIREFOX Mozilla Firefox CVE-2017-5459 WebGL Integer Overflow III	CVE-2017-5459	Browsers	3
BROWSER-FIREFOX Mozilla Firefox ReadableStreamCloseInternal out-of-bounds access attempt	CVE-2020-6806	Browsers	1
BROWSER-FIREFOX Mozilla Firefox Vorbis Audio Residue Codebook Out of Bounds Write CVE-2018-5146	CVE-2018-5146	Browsers	1
BROWSER-FIREFOX Mozilla Firefox domFuzzLite3 table use after free attempt	CVE-2017-5404	Browsers	1
BROWSER-FIREFOX Mozilla Firefox javascript type confusion code execution attempt	CVE-2018-12386	Browsers	2
BROWSER-FIREFOX Mozilla Firefox method	CVE-2018-	Browsers	2

array.prototype.push remote code execution attempt	12387		
BROWSER-FIREFOX Mozilla Firefox potential use after free attempt	CVE-2020-6819	Browsers	1
BROWSER-IE Microsoft Edge CVE-2016-3386 Spread Operator Memory Corruption Attempt	CVE-2016-3386	Browsers	2
BROWSER-IE Microsoft Edge CVE-2018-8556 bailOnImplicitCall Type Confusion Attempt	CVE-2018-8556	Browsers	3
BROWSER-IE Microsoft Edge CVE-2019-0648 Information Disclosure	CVE-2019-0648	Browsers	2
BROWSER-IE Microsoft Edge CVE-2019-0658 Information Disclosure	CVE-2019-0658	Browsers	1
BROWSER-IE Microsoft Edge CVE-2019-0676 Information Disclosure	CVE-2019-0676	Browsers	2
BROWSER-IE Microsoft Edge CVE-2019-0930 Information Disclosure	CVE-2019-0930	Browsers	2
BROWSER-IE Microsoft Edge Chakra CVE-2018-0780 AsmJSByteCodeGenerator EmitCall Type Confusion I	CVE-2018-0780	Browsers	1

BROWSER-IE Microsoft Edge Chakra Scripting Engine localeCompare type confusion attempt	CVE-2018-8355	Browsers	2
BROWSER-IE Microsoft Edge spread operator memory corruption attempt	CVE-2016-7296	Browsers	2
BROWSER-IE Microsoft Edge spread operator memory corruption attempt	CVE-2016-7297	Browsers	2
BROWSER-IE Microsoft Internet Explorer CAttrArray use after free attempt	CVE-2015-6143	Browsers	1
BROWSER-IE Microsoft Internet Explorer CVE-2016-7283 CWigglyShape Information Disclosure	CVE-2016-7283	Browsers	2
BROWSER-IE Microsoft Internet Explorer CVE-2016-7283 CWigglyShape Information Disclosure	CVE-2016-7283	Browsers	2
BROWSER-IE Microsoft Internet Explorer CVE-2018-8563 DirectX information disclosure attempt	CVE-2018-8563	Browsers	2
BROWSER-IE Microsoft Internet Explorer CVE-2019-0676 information disclosure attempt	CVE-2019-0676	Browsers	2

BROWSER-IE Microsoft Internet Explorer object use after free attempt	CVE-2017-8749	Browsers	1
BROWSER-IE Oracle Java Web Start arbitrary command execution attempt - Internet Explorer	CVE-2010-0886	Browsers	1
BROWSER-OTHER Apple Safari WebKit SVG Memory Corruption	CVE-2011-0222	Browsers	1
BROWSER-OTHER Apple Safari WebKit innerHTML Double Free Memory Corruption (Published Exploit)	CVE-2011-0221	Browsers	1
BROWSER-OTHER Cisco Webex Meetings Desktop App arbitrary program execution attempt	CVE-2020-3263	Browsers	1
BROWSER-OTHER Cisco Webex Teams URI scheme remote code execution attempt	CVE-2019-1636	Browsers	1
BROWSER-OTHER IBM Notes denial of service attempt	CVE-2017-1130	Browsers	2
BROWSER-OTHER Microsoft Edge CVE-2016-7206 Remote Code Execution Vulnerability	CVE-2016-7206	Browsers	1
BROWSER-OTHER	CVE-2010-	Browsers	2

Multiple Browser CVE-2010-3257 WebKit Stale Pointer Use-after-free Code Execution	3257		
BROWSER-OTHER Novell Messenger Client nim URI handler buffer overflow attempt	CVE-2013-1085	Browsers	1
BROWSER-OTHER Opera animation element denial of service attempt		Browsers	1
BROWSER-OTHER Opera browser window null pointer dereference attempt		Browsers	2
BROWSER-PLUGINS AOL IWinAmpActiveX class ConvertFile buffer overflow attempt		Browsers	1
BROWSER-PLUGINS Advantech WebAccess Node chkLogin2 SQL Injection CVE-2018-5443	CVE-2018-5443	Browsers	2
BROWSER-PLUGINS Advantech Webaccess webvrpcs Directory Traversal Remote Code Execution CVE-2017-16720	CVE-2017-16720	Browsers	2
BROWSER-PLUGINS Advantech Webaccess webvrpcs Directory Traversal Remote Code Execution CVE-2019-	CVE-2019-13552	Browsers	1

13552			
BROWSER-PLUGINS HP PoS CVE-2014-7890 OPOS Driver opostoneindicator.ocx Open Method Stack Overflow	CVE-2014-7890	Browsers	2
BROWSER-PLUGINS Microsoft Internet Explorer Dynamic Casts ActiveX clsid access	CVE-2006-3638	Browsers	2
BROWSER-PLUGINS Mitsubishi Electric E-Designer BEComliSlave Status_bit Stack Buffer Overflow	CVE-2017-9638	Browsers	3
BROWSER-PLUGINS Novell CVE-2011-4187 iPrint Client GetDriverSettings Realm Parameter Stack Buffer Overflow I	CVE-2011-4187	Browsers	3
BROWSER-PLUGINS Novell CVE-2011-4187 iPrint Client GetDriverSettings Realm Parameter Stack Buffer Overflow II	CVE-2011-4187	Browsers	3
BROWSER-PLUGINS Novell CVE-2011-4187 iPrint Client GetDriverSettings Realm Parameter Stack Buffer Overflow III	CVE-2011-4187	Browsers	3
BROWSER-PLUGINS Novell Messenger Client	CVE-2013-	Browsers	1

Filename Parameter Stack Buffer Overflow	1085		
BROWSER-PLUGINS Novell iPrint CVE-2009-1569 Client ienipp.ocx volatile-date-time Parsing Buffer Overflow	CVE-2009-1569	Browsers	2
BROWSER-PLUGINS Novell iPrint Client Browser Plugin call-back-url Buffer Overflow	CVE-2010-1527	Browsers	1
BROWSER-PLUGINS Novell iPrint Client ExecuteRequest debug Parameter Buffer Overflow		Browsers	1
BROWSER-PLUGINS Novell iPrint Client ExecuteRequest debug Parameter Buffer Overflow		Browsers	4
BROWSER-PLUGINS Novell iPrint Client GetDriverSettings Stack Buffer Overflow		Browsers	1
BROWSER-PLUGINS Novell iPrint Client GetDriverSettings Stack Buffer Overflow		Browsers	4
BROWSER-PLUGINS Novell iPrint Client ienipp.ocx target-frame Stack Buffer Overflow	CVE-2009-1568	Browsers	1

BROWSER-PLUGINS Oracle Java browser plugin docbase overflow attempt	CVE-2010-3552	Browsers	1
BROWSER-PLUGINS Trend Micro Control Manager ThreatDistributedTrail ThreatName SQL Injection CVE-2018-3606	CVE-2018-3606	Browsers	1
BROWSER-PLUGINS Trend Micro Control Manager sCloudService GetPassword SQL Injection CVE-2018-3604	CVE-2018-3604	Browsers	1
BROWSER-WEBKIT Apple Safari Browser putToPrimitive Cross-Site Scripting Attempt	CVE-2019-8764	Browsers	1
BROWSER-WEBKIT Apple Safari CSS font format corruption attempt	CVE-2010-0046	Browsers	1
BROWSER-WEBKIT Apple Safari CVE-2017-1684 Denial Of Service	CVE-2017-1684	Browsers	2
BROWSER-WEBKIT Apple Safari CVE-2017-2363 Same Origin Policy	CVE-2017-2363	Browsers	2
BROWSER-WEBKIT Apple Safari CVE-2017-2364 Universal Cross Site Scripting	CVE-2017-2364	Browsers	2

BROWSER-WEBKIT Apple Safari CVE-2017-2445 Universal Cross Site Scripting	CVE-2017-2445	Browsers	2
BROWSER-WEBKIT Apple Safari CVE-2017-2447 Denial Of Service	CVE-2017-2447	Browsers	2
BROWSER-WEBKIT Apple Safari CVE-2017-2479 Universal Cross Site Scripting	CVE-2017-2479	Browsers	2
BROWSER-WEBKIT Apple Safari CVE-2017-2521 Denial Of service	CVE-2017-2521	Browsers	2
BROWSER-WEBKIT Apple Safari CVE-2017-7037 Denial Of Service	CVE-2017-7037	Browsers	2
BROWSER-WEBKIT Apple Safari CVE-2017-7092 Denial Of service	CVE-2017-7092	Browsers	2
BROWSER-WEBKIT Apple Safari CVE-2017-7117 Denial Of Service	CVE-2017-2363	Browsers	1
BROWSER-WEBKIT Apple Safari CVE-2017-7117 Denial Of Service	CVE-2017-2363	Browsers	2
BROWSER-WEBKIT Apple Safari CVE-2018-4382 WebKit handleIntrinsicCall Type Confusion	CVE-2018-4382	Browsers	2
BROWSER-WEBKIT Apple Safari Same	CVE-2016-1697	Browsers	1

Origin Policy Bypass			
BROWSER-WEBKIT Apple Safari WebKit JavaScript engine type confusion attempt	CVE-2019-8820	Browsers	1
BROWSER-WEBKIT Apple Safari WebKit Out Of Bounds Write	CVE-2017-2505	Browsers	2
BROWSER-WEBKIT Apple Safari WebKit cached page memory corruption attempt	CVE-2019-8822	Browsers	2
BROWSER-WEBKIT Apple Safari WebKit memory corruption attempt	CVE-2018-4368	Browsers	1
BROWSER-WEBKIT Apple Safari WebKit out-of-bounds read attempt	CVE-2019-8689	Browsers	1
BROWSER-WEBKIT Apple Safari WebKit out-of-bounds write attempt	CVE-2017-2505	Browsers	1
BROWSER-WEBKIT Apple Safari Webkit CSS Charset Text transformation code execution attempt	CVE-2010-1770	Browsers	1
BROWSER-WEBKIT Apple Safari Webkit CVE-2012-1520 CSS Title Memory Corruption Attempt	CVE-2012-1520	Browsers	2

BROWSER-WEBKIT Apple Safari Webkit ContentEditable code execution attempt	CVE-2010-1396	Browsers	1
BROWSER-WEBKIT Apple Safari Webkit SVG memory corruption attempt	CVE-2011-0222	Browsers	1
BROWSER-WEBKIT Apple Safari Webkit WebCore memory corruption attempt	CVE-2018-4200	Browsers	2
BROWSER-WEBKIT Apple Safari Webkit attribute child removal code execution attempt	CVE-2010-1119	Browsers	1
BROWSER-WEBKIT Apple Safari Webkit floating point buffer overflow attempt	CVE-2009-2195	Browsers	1
BROWSER-WEBKIT Apple Safari Webkit floating point conversion memory corruption attempt	CVE-2010-1807	Browsers	1
BROWSER-WEBKIT Apple Safari WebkitCVE-2017-2464 Denial Of Service	CVE-2017-2464	Browsers	2
BROWSER-WEBKIT Apple Safari browser putToPrimitive cross-site scripting attempt	CVE-2019-8764	Browsers	1
BROWSER-WEBKIT	CVE-2018-	Browsers	1

Apple Safari memory corruption attempt	4443		
BROWSER-WEBKIT Apple WebKit JSArray component out-of-bounds access	CVE-2019-8518	Browsers	1
BROWSER-WEBKIT Apple WebKit QuickTime plugin CVE-2012-3753 content-type http header buffer overflow attempt	CVE-2012-3753	Browsers	2
BROWSER-WEBKIT Apple WebKit Same origin policy bypass	CVE-2016-1667	Browsers	1
BROWSER-WEBKIT Apple WebKit memory corruption attempt CVE-2018-4233	CVE-2018-4233	Browsers	1
BROWSER-WEBKIT Apple WebKit memory corruption attempt	CVE-2018-4233	Browsers	1
BROWSER-WEBKIT Apple WebKit updateReferencedText use-after-free attempt	CVE-2018-4315	Browsers	1
BROWSER-WEBKIT Apple Webkit CVE-2018-4318 SVGTextLayoutAttributes Use After Free	CVE-2018-4318	Browsers	2
BROWSER-WEBKIT Apple Webkit updateDescendantDependentFlags use-after-	CVE-2018-4317	Browsers	1

free attempt			
BROWSER-WEBKIT Apple Webkit updateMinimumColumnHeight use-after-free attempt	CVE-2018-4323	Browsers	2
BROWSER-WEBKIT Apple ioS WebKit Denial Of Service Vulnerability	CVE-2016-4622	Browsers	2
BROWSER-WEBKIT WebKit AudioArray allocate out of bounds access attempt	CVE-2020-3894	Browsers	1
BROWSER-WEBKIT WebKit CVE-2017-2470 Information Disclosure	CVE-2017-2470	Browsers	2
BROWSER-WEBKIT WebKit JavaScriptCore emitEqualityOpImpl memory corruption attempt	CVE-2019-8684	Browsers	1
BROWSER-WEBKIT WebKit JavaScriptCore emitEqualityOpImpl memory corruption attempt	CVE-2019-8684	Browsers	2
FILE-EXECUTABLE Microsoft Windows Win32k privilege escalation attempt	CVE-2018-8404	Application and Software	2
FILE-EXECUTABLE Symantec Antivirus CVE-2016-2208 Engine PE Header Heap Buffer	CVE-2016-2208	Application and Software	2

Overflow			
FILE-FLASH Adobe Adobe Flash Player ActionExtends use after free attempt	CVE-2016-7859	Multimedia	1
FILE-FLASH Adobe Flash AVC Decoder Memory Corruption attempt	CVE-2016-4275	Multimedia	1
FILE-FLASH Adobe Flash CVE-2016-0997 Remote Code Execution Vulnerability	CVE-2016-0997	Multimedia	2
FILE-FLASH Adobe Flash CVE-2016-4231 Use-After-Free Vulnerability	CVE-2016-4231	Multimedia	2
FILE-FLASH Adobe Flash ContextMenu Clone memory corruption vulnerability attempt	CVE-2016-4284	Multimedia	1
FILE-FLASH Adobe Flash MovieClip proto chain manipulation targeting constructor use after free attempt	CVE-2016-7865	Multimedia	1
FILE-FLASH Adobe Flash Player ABRControlParameters access memory corruption attempt	CVE-2016-4185	Multimedia	1
FILE-FLASH Adobe Flash Player AS2 setInterval use after free attempt	CVE-2016-0988	Multimedia	1
FILE-FLASH Adobe Flash	CVE-2016-	Multimedia	1

Player AS3 multiple axis attributes integer overflow attempt	0989		
FILE-FLASH Adobe Flash Player ASnative setFocus use after free attempt	CVE-2016-7864	Multimedia	1
FILE-FLASH Adobe Flash Player AVSegmentedSource use after free attempt	CVE-2016-7857	Multimedia	1
FILE-FLASH Adobe Flash Player BitmapData applyFilter integer overflow attempt	CVE-2016-7875	Multimedia	1
FILE-FLASH Adobe Flash Player BitmapData.applyFilter access violation attempt	CVE-2016-0961	Multimedia	1
FILE-FLASH Adobe Flash Player BitmapData.copyChannel access violation attempt	CVE-2016-0960	Multimedia	1
FILE-FLASH Adobe Flash Player BitmapData.paletteMap size mismatch integer overflow attempt	CVE-2016-0962	Multimedia	1
FILE-FLASH Adobe Flash Player ByteArray type confusion memory corruption attempt	CVE-2016-4249	Multimedia	1
FILE-FLASH Adobe Flash Player CVE-2013-3361	CVE-2013-	Multimedia	2

Remote Code Execution Vulnerability	3361		
FILE-FLASH Adobe Flash Player CVE-2014-8439 Remote Code Execution Vulnerability	CVE-2014-8439	Multimedia	2
FILE-FLASH Adobe Flash Player CVE-2015-3078 Remote Code Execution Vulnerability	CVE-2015-3078	Multimedia	2
FILE-FLASH Adobe Flash Player CVE-2015-5539 Remote Code Execution Vulnerability	CVE-2015-5539	Multimedia	2
FILE-FLASH Adobe Flash Player CVE-2015-5552 Remote Code Execution Vulnerability	CVE-2015-5552	Application and Software	1
FILE-FLASH Adobe Flash Player CVE-2016-1010 Rectangle Width Integer Overflow	CVE-2016-1010	Multimedia	1
FILE-FLASH Adobe Flash Player CVE-2016-4177 SceneAndFrameData Memory Corruption	CVE-2016-4177	Multimedia	2
FILE-FLASH Adobe Flash Player CVE-2016-4227 ActionScript setFocus Use After Free Attempt	CVE-2016-4227	Multimedia	2
FILE-FLASH Adobe Flash Player CVE-2016-4231 MovieClip method loop use-after-free	CVE-2016-4231	Multimedia	2

FILE-FLASH Adobe Flash Player CVE-2018-12824 Information Disclosure Vulnerability	CVE-2018-12827	Multimedia	2
FILE-FLASH Adobe Flash Player CVE-2018-12824 Information Disclosure Vulnerability	CVE-2018-12827	Multimedia	2
FILE-FLASH Adobe Flash Player CVE-2018-12826 Information Disclosure Vulnerability	CVE-2018-12826	Multimedia	2
FILE-FLASH Adobe Flash Player CVE-2018-15982 Use After Free I	CVE-2008-2992	Multimedia	2
FILE-FLASH Adobe Flash Player CVE-2018-15982 Use After Free II	CVE-2008-2992	Multimedia	2
FILE-FLASH Adobe Flash Player CVE-2018-15982 Use After Free	CVE-2008-2992	Multimedia	2
FILE-FLASH Adobe Flash Player CVE-2018-5000 Memory Address Disclosure	CVE-2018-5000	Multimedia	1
FILE-FLASH Adobe Flash Player Camera use after free attempt	CVE-2017-3003	Multimedia	1
FILE-FLASH Adobe Flash Player DRMManager memory corruption attempt	CVE-2016-4285	Multimedia	1
FILE-FLASH Adobe Flash	CVE-2016-	Multimedia	1

Player DefineBitsJPEG2 invalid length memory corruption attempt	4179		
FILE-FLASH Adobe Flash Player DisplacementMapFilter use-after-free attempt	CVE-2016-4272	Multimedia	1
FILE-FLASH Adobe Flash Player ExportAssets count memory corruption attempt	CVE-2016-1012	Multimedia	1
FILE-FLASH Adobe Flash Player FrameLabel memory corruption attempt	CVE-2016-6986	Multimedia	1
FILE-FLASH Adobe Flash Player JPEG handling memory corruption attempt	CVE-2016-4229	Multimedia	1
FILE-FLASH Adobe Flash Player LocaleID determinePreferredLocales Out-Of-Bounds Access	CVE-2017-3114	Multimedia	1
FILE-FLASH Adobe Flash Player LocaleID determinePreferredLocales Out-Of-Bounds Access	CVE-2017-3114	Multimedia	4
FILE-FLASH Adobe Flash Player MPD use-after-free attempt	CVE-2016-1006	Multimedia	1
FILE-FLASH Adobe Flash Player Malformed ATF	CVE-2016-1002	Application and Software	1

Heap Overflow Attempt			
FILE-FLASH Adobe Flash Player MediaPlayerItemLoader out of bounds memory access attempt	CVE-2016-4182	Multimedia	1
FILE-FLASH Adobe Flash Player MovieClip method loop use-after-free attempt CVE-2016-4231	CVE-2016-4231	Multimedia	2
FILE-FLASH Adobe Flash Player MovieClip method use after free attempt	CVE-2015-8639	Multimedia	1
FILE-FLASH Adobe Flash Player NetConnection proxyType invalid value out of bounds read attempt	CVE-2016-7874	Multimedia	1
FILE-FLASH Adobe Flash Player NetConnection use after free attempt	CVE-2016-7879	Multimedia	1
FILE-FLASH Adobe Flash Player NetStream type confusion attempt	CVE-2016-4280	Multimedia	1
FILE-FLASH Adobe Flash Player Primetime SDK out of bounds read attempt	CVE-2016-7873	Multimedia	1
FILE-FLASH Adobe Flash Player QOSProvider use-after-free attempt	CVE-2016-6984	Multimedia	1

FILE-FLASH Adobe Flash Player Rectangle constructor use after free attempt	CVE-2016-4228	Multimedia	1
FILE-FLASH Adobe Flash Player ShimContentResolver out of bounds memory access attempt	CVE-2016-4283	Multimedia	1
FILE-FLASH Adobe Flash Player Stage align use aftre free attempt	CVE-2016-4226	Multimedia	2
FILE-FLASH Adobe Flash Player StyleSheets use after free attempt	CVE-2016-4174	Multimedia	1
FILE-FLASH Adobe Flash Player TextField use after free attempt	CVE-2016-7863	Multimedia	1
FILE-FLASH Adobe Flash Player TimedEvent memory corruption attempt	CVE-2016-4188	Multimedia	1
FILE-FLASH Adobe Flash Player Transform getter use after free attempt	CVE-2016-4230	Multimedia	1
FILE-FLASH Adobe Flash Player Transform object use after free attempt	CVE-2016-4173	Multimedia	1
FILE-FLASH Adobe Flash Player addCallback use after free attempt	CVE-2016-7858	Multimedia	1
FILE-FLASH Adobe Flash Player addProperty use	CVE-2016-7872	Multimedia	1

after free attempt			
FILE-FLASH Adobe Flash Player allocator use-after-free attempt	CVE-2017-3062	Multimedia	1
FILE-FLASH Adobe Flash Player and AIR Multiple Unspecified Memory Corruption Vulnerabilities	CVE-2015-3093	Multimedia	2
FILE-FLASH Adobe Flash Player determinePreferredLocales memory corruption attempt	CVE-2017-3114	Multimedia	2
FILE-FLASH Adobe Flash Player determinePreferredLocales out of bounds memory read attempt	CVE-2017-3082	Multimedia	1
FILE-FLASH Adobe Flash Player display list structure Memory Corruption Attempt	CVE-2017-2930	Web Services and Applications	1
FILE-FLASH Adobe Flash Player duplicateMovieClip use after free attempt	CVE-2016-1013	Multimedia	1
FILE-FLASH Adobe Flash Player event handler out of bounds memory access attempt	CVE-2016-6985	Multimedia	1
FILE-FLASH Adobe Flash Player hitTest BitmapData object integer overflow	CVE-2016-0963	Multimedia	1

attempt			
FILE-FLASH Adobe Flash Player htmlText method use-after-free memory corruption attempt	CVE-2016-0995	Multimedia	1
FILE-FLASH Adobe Flash Player invalid FLV header out of bounds write attempt	CVE-2016-1001	Multimedia	1
FILE-FLASH Adobe Flash Player malformed ATF file length heap overflow attempt	CVE-2017-2934	Multimedia	1
FILE-FLASH Adobe Flash Player malformed ActionSetTarget record information disclosure attempt	CVE-2018-5008	Multimedia	2
FILE-FLASH Adobe Flash Player malformed PlaceObject3 memory corruption attempt	CVE-2017-2931	Multimedia	1
FILE-FLASH Adobe Flash Player malformed VideoFrame memory corruption attempt	CVE-2016-4274	Multimedia	1
FILE-FLASH Adobe Flash Player malformed regular expression use after free attempt	CVE-2016-4121	Multimedia	2
FILE-FLASH Adobe Flash Player malformed tag out of bounds read attempt	CVE-2016-4176	Multimedia	1

FILE-FLASH Adobe Flash Player multiple scripts display rendering use-after-free attempt	CVE-2016-1011	Multimedia	1
FILE-FLASH Adobe Flash Player newfunction memory corruption exploit attempt	CVE-2010-0197	Multimedia	1
FILE-FLASH Adobe Flash Player onSetFocus movie clip use after free attempt	CVE-2016-7892	Multimedia	1
FILE-FLASH Adobe Flash Player onSetFocus movieclip use after free attempt	CVE-2017-2932	Multimedia	1
FILE-FLASH Adobe Flash Player out of bounds memory access attempt	CVE-2016-4281	Multimedia	1
FILE-FLASH Adobe Flash Player out of scope newclass memory corruption attempt	CVE-2015-0322	Multimedia	1
FILE-FLASH Adobe Flash Player rectangle width integer overflow attempt	CVE-2016-1010	Multimedia	1
FILE-FLASH Adobe Flash Player recursion calls stack overflow attempt	CVE-2016-0986	Multimedia	1
FILE-FLASH Adobe Flash Player recursive doaction stack exhaustion	CVE-2011-2457	Multimedia	1

FILE-FLASH Adobe Flash Player sentEvent use after free attempt	CVE-2016-6987	Multimedia	1
FILE-FLASH Adobe Flash Player si32 integer overflow attempt	CVE-2016-0993	Multimedia	1
FILE-FLASH Adobe Flash Player swapDepths use after free attempt	CVE-2016-0999	Multimedia	1
FILE-FLASH Adobe Flash Player toString type confusion memory corruption attempt	CVE-2016-1019	Multimedia	1
FILE-FLASH Adobe Flash Player use after free attempt	CVE-2016-0987	Multimedia	1
FILE-FLASH Adobe Flash Player visual blend out of bounds read attempt	CVE-2017-2928	Multimedia	1
FILE-FLASH Adobe Flash Player writeDynamicProperties use-after-free attempt	CVE-2016-7877	Multimedia	1
FILE-FLASH Adobe Primetime SDK setObject type confusion attempt	CVE-2016-7861	Multimedia	1
FILE-FLASH Adobe Reader CVE-2013-5324 Remote Code Execution	CVE-2013-5324	Multimedia	2
FILE-FLASH Adobe Standalone Flash Player AS3 NetStream object	CVE-2016-6981	Multimedia	1

use after free attempt			
FILE-FLASH Adobe Standalone Flash Player AS3 Primetime timeline ShimContentResolver out of bounds read attempt	CVE-2016-6983	Multimedia	1
FILE-FLASH Adobe Standalone Flash Player ASnative object use after free attempt	CVE-2016-0991	Multimedia	1
FILE-FLASH Adobe Standalone Flash Player PSDK FlashRuntime mediaplayer pause attempt	CVE-2016-6982	Multimedia	1
FILE-FLASH Adobe Standalone Flash Player out of bounds memory access attempt	CVE-2016-4282	Multimedia	1
FILE-FLASH Adobe Standalone Flash Player texfield getter use after free attempt	CVE-2016-0990	Multimedia	1
FILE-FLASH Adobe Standalone Flash Player use after free attempt	CVE-2016-4279	Multimedia	1
FILE-IDENTIFY .rtx file attachment detected		Application and Software	4
FILE-IDENTIFY Apple QuickTime PICT v2.0 Image header	CVE-2011-0257	Application and Software	4
FILE-IDENTIFY Apple		Application	4

Quicktime Targa Image file download request		and Software	
FILE-IDENTIFY EPS file download request		Application and Software	4
FILE-IDENTIFY FlashPix file download request		Application and Software	4
FILE-IDENTIFY Heroes of Might and Magic III map file download request		Application and Software	4
FILE-IDENTIFY ISO file download request		Application and Software	4
FILE-IDENTIFY JNLP file attachment detected		Application and Software	4
FILE-IDENTIFY Java .class file download request		Application and Software	4
FILE-IDENTIFY MachO x64 Little Endian file magic detected		Application and Software	4
FILE-IDENTIFY Oracle Java JMX management loading mlet detected		Application and Software	4
FILE-IDENTIFY RAR file magic detected		Application and Software	4
FILE-IDENTIFY RMF file attachment detected		Application and Software	4
FILE-IDENTIFY RSS file download request		Application and Software	4
FILE-IDENTIFY SMIL file		Application	4

download request		and Software	
FILE-IDENTIFY SVG file download request		Application and Software	4
FILE-IDENTIFY XBM image file download request		Application and Software	4
FILE-IDENTIFY maplet bin file download attempt		Application and Software	4
FILE-IDENTIFY maplet file attachment detected		Application and Software	4
FILE-IMAGE Acrobat Reader CVE-2018-5058 Information Disclosure Vulnerability	CVE-2018-5058	Multimedia	1
FILE-IMAGE Acrobat Reader CVE-2018-5058 Information Disclosure Vulnerability	CVE-2018-5058	Multimedia	1
FILE-IMAGE Adobe Acrobat TIFF ICC tag heap buffer overflow attempt	CVE-2017-2963	Multimedia	1
FILE-IMAGE Adobe Acrobat TIFF PhotometricInterpretation heap buffer overflow attempt	CVE-2017-2966	Multimedia	1
FILE-IMAGE Adobe Acrobat TIFF Software tag heap buffer overflow attempt	CVE-2017-2965	Multimedia	2

FILE-IMAGE Adobe Photoshop CS5 gif file heap corruption attempt	CVE-2011-2131	Multimedia	1
FILE-IMAGE Adobe Pro DC Exif ModifyDate metadata memory corruption attempt	CVE-2016-1076	Multimedia	1
FILE-IMAGE Adobe Pro DC Exif Software metadata memory corruption attempt	CVE-2016-1076	Multimedia	1
FILE-IMAGE Adobe Reader malformed app13 marker memory corruption attempt	CVE-2017-2964	Multimedia	1
FILE-IMAGE Apple QuickTime Targa image file buffer overflow attempt	CVE-2012-3755	Multimedia	1
FILE-IMAGE Apple Quicktime FlashPix processing overflow attempt	CVE-2009-2798	Multimedia	1
FILE-IMAGE Apple Quicktime malformed FPX file memory corruption attempt	CVE-2016-1767	Multimedia	2
FILE-IMAGE Apple Quicktime malformed FPX file memory corruption attempt	CVE-2016-1768	Multimedia	2
FILE-IMAGE ImageMagick LibTIFF	CVE-2016-8707	Multimedia	3

invalid SamplesPerPixel buffer overflow attempt			
FILE-IMAGE ImageMagick PostScript decode delegate command injection attempt		Multimedia	1
FILE-IMAGE ImageMagick SGI File Handling Buffer Overflow	CVE-2018-5040	Multimedia	2
FILE-IMAGE ImageMagick WWWDecodeDelegate command injection attempt	CVE-2016-3714	Multimedia	1
FILE-IMAGE ImageMagick WWWDecodeDelegate command injection attempt	CVE-2016-3714	Multimedia	2
FILE-IMAGE ImageMagick and GraphicsMagick OpenBlob command injection attempt	CVE-2016-5118	Multimedia	1
FILE-IMAGE OpenOffice EMF file EMR record parsing integer overflow attempt	CVE-2008-2238	Multimedia	1
FILE-IMAGE Oracle Java Web Start Splashscreen GIF decoding buffer overflow attempt	CVE-2008-2086	Multimedia	1

FILE-JAVA Oracle Java 2D ImagingLib AffineTransformOp integer overflow attempt	CVE-2013-0809	Application and Software	1
FILE-JAVA Oracle Java 2D ImagingLib AffineTransformOp storeImageArray memory corruption attempt	CVE-2013-2465	Application and Software	1
FILE-JAVA Oracle Java 2D ImagingLib ConvolveOp integer overflow attempt	CVE-2013-0809	Application and Software	1
FILE-JAVA Oracle Java 2D ImagingLib LookupOp integer overflow attempt	CVE-2013-0809	Application and Software	1
FILE-JAVA Oracle Java Applet Rhino script engine remote code execution attempt	CVE-2011-3544	Application and Software	2
FILE-JAVA Oracle Java Applet remote code execution attempt	CVE-2011-3544	Application and Software	1
FILE-JAVA Oracle Java AtomicReferenceFieldUpdater remote code execution attempt	CVE-2014-4262	Application and Software	1
FILE-JAVA Oracle Java CVE-2010-4462 XGetSamplePtrFromSnd Memory Corruption Attempt	CVE-2010-4462	Application and Software	2

FILE-JAVA Oracle Java CVE-2011-0802 FileDialog.Show Heap Buffer Overflow	CVE-2011-0802	Application and Software	2
FILE-JAVA Oracle Java CVE-2011-3545 MixerSequencer.nAddControllerEventCallback Array Index Out-of-bounds	CVE-2011-3545	Application and Software	2
FILE-JAVA Oracle Java CVE-2012-0500 Web Start Arbitrary Command Execution Attempt	CVE-2012-0500	Application and Software	1
FILE-JAVA Oracle Java CVE-2013-2470, sun.awt.image.ImagingLib.lookupByteBI Memory Corruption	CVE-2013-2470	Application and Software	3
FILE-JAVA Oracle Java CVE-2013-2473 java.awt.image.ByteComponentRaster Memory Corruption	CVE-2013-2473	Application and Software	2
FILE-JAVA Oracle Java HsbParser.getSoundBank stack buffer overflow attempt	CVE-2009-3867	Application and Software	1
FILE-JAVA Oracle Java ImagingLib buffer overflow attempt	CVE-2013-2463	Application and Software	1
FILE-JAVA Oracle Java ImagingLib buffer overflow attempt	CVE-2013-2463	Application and Software	2

FILE-JAVA Oracle Java IntegerInterleavedRaster integer overflow attempt	CVE-2013-2471	Application and Software	1
FILE-JAVA Oracle Java IntegerInterleavedRaster.verify method integer overflow attempt	CVE-2013-2471	Application and Software	1
FILE-JAVA Oracle Java JMX class arbitrary code execution attempt	CVE-2013-0422	Application and Software	1
FILE-JAVA Oracle Java PhantomReference CVE-2015-0395 Use After Free	CVE-2015-0395	Application and Software	2
FILE-JAVA Oracle Java Rhino script engine remote code execution attempt	CVE-2011-3544	Application and Software	1
FILE-JAVA Oracle Java Runtime AWT setDiffICM stack buffer overflow attempt	CVE-2009-3869	Application and Software	1
FILE-JAVA Oracle Java Runtime CVE-2012-1723 Bytecode Verifier Cache Code Execution	CVE-2012-1723	Application and Software	2
FILE-JAVA Oracle Java Runtime Environment CVE-2008-5352 Pack200 Decompression Integer Overflow attempt Vulnerability	CVE-2008-5352	Application and Software	1
FILE-JAVA Oracle Java	CVE-2008-	Application	1

Runtime Environment JAR File Processing Stack Buffer Overflow	5354	and Software	
FILE-JAVA Oracle Java Runtime Environment Pack200 Decompression Integer Overflow attempt	CVE-2008-5352	Application and Software	1
FILE-JAVA Oracle Java Runtime Environment Pack200 Decompression Integer Overflow	CVE-2009-1095	Application and Software	1
FILE-JAVA Oracle Java Runtime true type font idef opcode heap buffer overflow attempt	CVE-2012-0499	Application and Software	1
FILE-JAVA Oracle Java ShortComponentRaster integer overflow attempt	CVE-2013-2472	Application and Software	1
FILE-JAVA Oracle Java System.arraycopy race condition attempt	CVE-2014-0456	Application and Software	1
FILE-JAVA Oracle Java Web Start JNLP j2se key value buffer overflow attempt	CVE-2008-3111	Application and Software	1
FILE-JAVA Oracle Java XGetSamplePtrFromSnd memory corruption attempt	CVE-2010-4462	Application and Software	1
FILE-JAVA Oracle Java and JavaFX JPEGImageReader memory corruption	CVE-2013-2420	Application and Software	1

attempt			
FILE-JAVA Oracle Java browser plugin docbase overflow attempt	CVE-2010-3552	Application and Software	1
FILE-JAVA Oracle Java field bytecode verifier cache code execution attempt	CVE-2012-1723	Application and Software	1
FILE-JAVA Oracle Java font rendering remote code execution attempt	CVE-2013-1491	Application and Software	1
FILE-JAVA Oracle Java getSoundBank overflow Attempt malicious jar file	CVE-2009-3867	Application and Software	1
FILE-JAVA Oracle Java java.util.concurrent.ConcurrentHashMap memory corruption attempt	CVE-2013-2426	Application and Software	1
FILE-JAVA Oracle Java sun.awt.image.ImageRepresentation.setPixels integer overflow attempt	CVE-2013-2420	Application and Software	1
FILE-JAVA Oracle Java sun.awt.image.ImagingLib.lookupByteBI memory corruption attempt	CVE-2013-2470	Application and Software	1
FILE-MULTIMEDIA Adobe Flash Player MP4 stsz atom memory corruption attempt	CVE-2017-2926	Multimedia	1

FILE-MULTIMEDIA Apple QuickTime CVE-2011-0257 PICT Image PnSize Opcode Stack Buffer Overflow	CVE-2011-0257	Multimedia	2
FILE-MULTIMEDIA Apple QuickTime FPX File Requested		Multimedia	4
FILE-MULTIMEDIA Apple QuickTime H.264 Movie File Buffer Overflow	CVE-2009-2799	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime Image Description Atom Sign Extension Memory Corruption	CVE-2009-0955	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime Image Description Atom Sign Extension Memory Corruption	CVE-2009-0955	Multimedia	4
FILE-MULTIMEDIA Apple QuickTime Image Description Atom sign extension memory corruption attempt	CVE-2009-0955	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime JPEG 2000 COD Length Integer Underflow	CVE-2011-3250	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime Movie File Clipping Region Handling Heap Buffer Overflow	CVE-2009-0954	Multimedia	1

FILE-MULTIMEDIA Apple QuickTime PDAT Atom parsing buffer overflow attempt	CVE-2008-3625	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime PICT File Processing Memory Corruption	CVE-2012-0671	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime PICT File Processing Memory Corruption	CVE-2012-0671	Multimedia	4
FILE-MULTIMEDIA Apple QuickTime PICT Image paintPoly Parsing Heap Buffer Overflow	CVE-2009-0010	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime PICT Image paintPoly Parsing Heap Buffer Overflow	CVE-2009-0010	Multimedia	4
FILE-MULTIMEDIA Apple QuickTime Plugin SetLanguage Buffer Overflow	CVE-2012-0666	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime Plugin SetLanguage Buffer Overflow	CVE-2012-0666	Multimedia	4
FILE-MULTIMEDIA Apple QuickTime QTPlugin.ocx _Marshaled_pUnk Code Execution		Multimedia	1
FILE-MULTIMEDIA Apple QuickTime QTPlugin.ocx		Multimedia	4

_Marshaled_pUnk Code Execution			
FILE-MULTIMEDIA Apple QuickTime QTVR QTVRStringAtom Parsing Buffer Overflow	CVE-2012-0667	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime QTVR QTVRStringAtom Parsing Buffer Overflow	CVE-2012-0667	Multimedia	4
FILE-MULTIMEDIA Apple QuickTime STSD JPEG atom heap corruption attempt	CVE-2009-0007	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime TeXML Color String Parsing Buffer Overflow	CVE-2012-0663	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime TeXML Color String Parsing Buffer Overflow	CVE-2012-0663	Multimedia	4
FILE-MULTIMEDIA Apple QuickTime TeXML Style Element Text Specification Buffer Overflow	CVE-2012-3752	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime TeXML Style Element Text Specification Buffer Overflow	CVE-2012-3752	Multimedia	4
FILE-MULTIMEDIA Apple QuickTime TeXML Transform Attribute	CVE-2012-0663	Multimedia	4

Parsing Buffer Overflow			
FILE-MULTIMEDIA Apple QuickTime TeXML textBox Element Memory Corruption	CVE-2013-1015	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime TeXML textBox Element Memory Corruption	CVE-2013-1015	Multimedia	4
FILE-MULTIMEDIA Apple QuickTime alis Volume Name Parsing Stack Buffer Overflow (Published Exploit)	CVE-2013-1017	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime enof Atom Parsing Heap Buffer Overflow	CVE-2013-0986	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime enof atom parsing heap buffer overflow attempt	CVE-2013-0986	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime ftab Atom Stack Buffer Overflow	CVE-2014-1246	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime marshaled punk remote code execution	CVE-2010-1818	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime movie file clipping region handling heap buffer overflow attempt	CVE-2009-0954	Multimedia	1

FILE-MULTIMEDIA Apple QuickTime pict image poly structure memory corruption attempt	CVE-2007-4676	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime streaming debug error logging buffer overflow attempt	CVE-2010-1799	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime text track descriptors heap buffer overflow attempt	CVE-2012-0664	Multimedia	1
FILE-MULTIMEDIA Apple QuickTime udta Atom Buffer Overflow		Multimedia	4
FILE-MULTIMEDIA Apple Quicktime MJPEG Frame stsd Atom Heap Overflow	CVE-2013-1020	Multimedia	1
FILE-MULTIMEDIA Apple Quicktime MJPEG Frame stsd Atom Heap Overflow	CVE-2013-1020	Multimedia	4
FILE-MULTIMEDIA Apple Quicktime Text Track Descriptors Heap Buffer Overflow	CVE-2012-0664	Multimedia	1
FILE-MULTIMEDIA Apple Quicktime Text Track Descriptors Heap Buffer Overflow	CVE-2012-0664	Multimedia	4
FILE-MULTIMEDIA Apple iTunes DAAP protocol handler stack buffer	CVE-2009-0950	Multimedia	1

overflow attempt			
FILE-MULTIMEDIA Apple iTunes ITMS protocol handler stack buffer overflow attempt	CVE-2009-0950	Multimedia	1
FILE-MULTIMEDIA Apple iTunes ITMSS protocol handler stack buffer overflow attempt	CVE-2009-0950	Multimedia	1
FILE-MULTIMEDIA Apple iTunes ITPC protocol handler stack buffer overflow attempt	CVE-2009-0950	Multimedia	1
FILE-MULTIMEDIA Apple iTunes Protocol Handler Stack Buffer Overflow	CVE-2009-0950	Multimedia	1
FILE-MULTIMEDIA RealNetworks CVE-2007-5081 RealPlayer RealMedia File Format Processing Heap Corruption Attempt	CVE-2007-5081	Multimedia	4
FILE-MULTIMEDIA RealNetworks RealPlayer IVR Handling Heap Buffer Overflow (Published Exploit)		Multimedia	4
FILE-OFFICE Adobe Acrobat ImageConversion JPEG Heap-based Buffer Overflow	CVE-2017-2959	Office Tools	1
FILE-OFFICE Adobe Acrobat ImageConversion JPEG	CVE-2017-2959	Office Tools	4

Heap-based Buffer Overflow			
FILE-OFFICE Adobe Acrobat ImageConversion JPEG Out-of-Bounds Read	CVE-2017-2960	Office Tools	1
FILE-OFFICE Adobe Acrobat ImageConversion JPEG Out-of-Bounds Read	CVE-2017-2960	Office Tools	4
FILE-OFFICE Adobe Acrobat ImageConversion TIFF Heap-based Buffer Overflow	CVE-2017-2966	Office Tools	4
FILE-OFFICE LibreOffice CVE-2018-6871 WEBSERVICE Information Disclosure	CVE-2018-6871	Office Tools	2
FILE-OFFICE LibreOffice LibreLogo Arbitrary Code Execution	CVE-2019-9848	Office Tools	1
FILE-OFFICE LibreOffice LibreLogo Arbitrary Code Execution	CVE-2019-9848	Office Tools	4
FILE-OFFICE LibreOffice Macro Event Remote Code Execution	CVE-2018-16858	Office Tools	2
FILE-OFFICE LibreOffice Macro Event Remote Code Execution	CVE-2018-16858	Office Tools	4
FILE-OFFICE Microsoft Office Excel CVE-2019-	CVE-2019-1112	Office Tools	2

1112 Information Disclosure			
FILE-OFFICE Microsoft Office Excel Information Disclosure Vulnerability CVE-2019-1110	CVE-2018-4901	Office Tools	1
FILE-OTHER ACD Systems ACDSee Products XBM file handling buffer overflow attempt		Application and Software	1
FILE-OTHER AOL Desktop RTX file parsing buffer overflow attempt		Application and Software	1
FILE-OTHER Acrobat Reader CVE-2018-12761 Information Disclosure Vulnerability	CVE-2018-12761	Application and Software	1
FILE-OTHER Acrobat Reader CVE-2018-12833 Information Disclosure Vulnerability	CVE-2018-12833	Application and Software	2
FILE-OTHER Acrobat Reader CVE-2018-12838 Information Disclosure Vulnerability	CVE-2018-12838	Application and Software	2
FILE-OTHER Acrobat Reader CVE-2018-12845 Information Disclosure Vulnerability	CVE-2018-12845	Application and Software	2
FILE-OTHER Acrobat Reader CVE-2018-12856 Information Disclosure Vulnerability	CVE-2018-12856	Application and Software	2

FILE-OTHER Acrobat Reader CVE-2018-15935 Information Disclosure Vulnerability	CVE-2018-15935	Application and Software	2
FILE-OTHER Acrobat Reader CVE-2018-15948 Information Disclosure Vulnerability	CVE-2018-15948	Application and Software	2
FILE-OTHER Acrobat Reader CVE-2018-5062 Information Disclosure Vulnerability	CVE-2018-5062	Application and Software	1
FILE-OTHER Acrobat Reader CVE-2018-5062 Information Disclosure Vulnerability	CVE-2018-5062	Application and Software	1
FILE-OTHER Acrobat Reader CVE-2018-5067 Information Disclosure Vulnerability	CVE-2018-5067	Application and Software	1
FILE-OTHER Acrobat Reader CVE-2018-5067 Information Disclosure Vulnerability	CVE-2018-5067	Application and Software	1
FILE-OTHER Acrobat Reader CVE-2019-7140 Out-of-Bound Read Vulnerability	CVE-2019-7140	Application and Software	2
FILE-OTHER Acrobat Reader CVE-2019-7143 Out-of-Bound Read Vulnerability	CVE-2019-7143	Application and Software	2
FILE-OTHER Acrobat Reader CVE-2019-7785	CVE-2019-7785	Application and Software	2

Use After Free Vulnerability			
FILE-OTHER Acrobat Reader CVE-2019-7787 Out-of-Bound Read Vulnerability	CVE-2019-7787	Application and Software	2
FILE-OTHER Acrobat Reader CVE-2019-7788 Use After Free Vulnerability	CVE-2019-7788	Application and Software	2
FILE-OTHER Acrobat Reader CVE-2019-7791 Use After Free Vulnerability	CVE-2019-7791	Application and Software	2
FILE-OTHER Acrobat Reader CVE-2019-7798 Out-of-Bound Read Vulnerability	CVE-2019-7798	Application and Software	2
FILE-OTHER Acrobat Reader CVE-2019-7799 Out-of-Bound Read Vulnerability	CVE-2019-7799	Application and Software	2
FILE-OTHER Acrobat Reader CVE-2019-7810 Out Of Bound Read Vulnerability	CVE-2019-7810	Application and Software	2
FILE-OTHER Acrobat Reader CVE-2019-7819 Use After Free Vulnerability	CVE-2019-7819	Application and Software	2
FILE-OTHER Acrobat Reader CVE-2019-7824 Buffer Error Vulnerability	CVE-2019-7824	Application and Software	2

FILE-OTHER Acrobat Reader CVE-2019-7825 Out-of-Bound Read Vulnerability	CVE-2019-7825	Application and Software	2
FILE-OTHER Adobe Acrobat And Reader EPS CVE-2018-12841 Arbitrary Code Execution	CVE-2018-12841	Application and Software	2
FILE-OTHER Adobe Acrobat CVE-2017-16395 EMF conversion heap buffer overflow attempt	CVE-2014-0529	Application and Software	2
FILE-OTHER Adobe Acrobat CVE-2017-16404 EMFPlus out of bounds buffer overflow attempt	CVE-2017-16404	Application and Software	2
FILE-OTHER Adobe Acrobat CVE-2017-16407 ImageConversion EMF BMP Out of Bounds Read II	CVE-2017-16407	Application and Software	1
FILE-OTHER Adobe Acrobat CVE-2017-16407 ImageConversion EMF BMP Out of Bounds Read	CVE-2017-16407	Application and Software	1
FILE-OTHER Adobe Acrobat CVE-2018-15934 Out Of Bounds Read	CVE-2018-15934	Application and Software	2
FILE-OTHER Adobe Acrobat CVE-2018-	CVE-2018-15986	Application and Software	2

15986 Memory Corruption			
FILE-OTHER Adobe Acrobat CVE-2019-7040 use after free attempt	CVE-2019-7040	Application and Software	2
FILE-OTHER Adobe Acrobat CVE-2019-7043 use after free attempt	CVE-2019-7043	Application and Software	2
FILE-OTHER Adobe Acrobat EMF EMR_CREATEMONOBRUSH out-of-bounds write attempt	CVE-2018-16020	Application and Software	2
FILE-OTHER Adobe Acrobat EMF embedded DIB out of bound read attempt	CVE-2018-4968	Application and Software	1
FILE-OTHER Adobe Acrobat EMF file GIF LZW coding table memory corruption attempt	CVE-2017-11258	Application and Software	2
FILE-OTHER Adobe Acrobat EMF file GIF sub-block memory corruption attempt	CVE-2017-11260	Application and Software	2
FILE-OTHER Adobe Acrobat EMF file kerning data memory corruption attempt	CVE-2017-11239	Application and Software	2
FILE-OTHER Adobe Acrobat EMF malformed Object record out-of-bounds	CVE-2018-4885	Application and Software	1

access attempt			
FILE-OTHER Adobe Acrobat EMF out of bounds read attempt	CVE-2018-16017	Application and Software	1
FILE-OTHER Adobe Acrobat EMF out-of-bounds read attempt	CVE-2018-16022	Application and Software	2
FILE-OTHER Adobe Acrobat EMF with malformed embedded JPEG memory corruption attempt	CVE-2017-11259	Application and Software	2
FILE-OTHER Adobe Acrobat HTML invalid pointer CVE-2018-12778 Out-Of-Bounds Read	CVE-2018-12778	Application and Software	2
FILE-OTHER Adobe Acrobat ImageConversion EMF EMR_STRETCHBLT Out of Bounds Read	CVE-2018-4886	Application and Software	3
FILE-OTHER Adobe Acrobat ImageConversion EMF EMR_STRETCHDIBITS Heap-based Buffer Overflow	CVE-2017-16397	Application and Software	2
FILE-OTHER Adobe Acrobat ImageConversion EMF EmfPlus Heap-based Buffer Overflow	CVE-2017-16416	Application and Software	2
FILE-OTHER Adobe Acrobat Index CVE-	CVE-2018-	Application	2

2018-4984 Out of Bounds	4984	and Software	
FILE-OTHER Adobe Acrobat JavaScript engine security bypass attempt	CVE-2019-7041	Application and Software	2
FILE-OTHER Adobe Acrobat PostScript file parsing TBuildCharDict use after free attempt	CVE-2019-7084	Application and Software	2
FILE-OTHER Adobe Acrobat Pro CVE-2018-15993 WebCapture use after free attempt	CVE-2018-15993	Application and Software	2
FILE-OTHER Adobe Acrobat Pro CVE-2018-19704 XPS file image-load out-of-bounds read attempt	CVE-2018-19704	Application and Software	2
FILE-OTHER Adobe Acrobat Pro CVE-2018-4893 XPS Out Of Bounds Read Attempt	CVE-2018-4893	Application and Software	2
FILE-OTHER Adobe Acrobat Pro CVE-2018-4896 Out Of Bounds Read Attempt	CVE-2018-4896	Application and Software	2
FILE-OTHER Adobe Acrobat Pro CVE-2018-4904 Embedded TIFF Heap Overflow Attempt I	CVE-2018-4904	Application and Software	2
FILE-OTHER Adobe Acrobat Pro CVE-2018-4904 Embedded TIFF	CVE-2018-4904	Application and Software	2

Heap Overflow Attempt II			
FILE-OTHER Adobe Acrobat Pro EMF Alphablend memory corruption attempt	CVE-2018-12789	Application and Software	2
FILE-OTHER Adobe Acrobat Pro EMF CVE-2018-4986 Sensitive Information Disclosure	CVE-2018-4986	Application and Software	3
FILE-OTHER Adobe Acrobat Pro EMF EmfPlusDrawString out of bounds read attempt	CVE-2018-4879	Application and Software	2
FILE-OTHER Adobe Acrobat Pro EMF ImageConversion out-of-bounds write attempt	CVE-2018-12860	Application and Software	2
FILE-OTHER Adobe Acrobat Pro EMF file EMR_ALPHABLEND record memory corruption attempt		Application and Software	1
FILE-OTHER Adobe Acrobat Pro EMF file out-of-bounds write attempt	CVE-2018-12865	Application and Software	2
FILE-OTHER Adobe Acrobat Pro EMF malformed bitmap rectangle destination out of bounds read attempt	CVE-2018-4886	Application and Software	1

FILE-OTHER Adobe Acrobat Pro EMF malformed bitmap rectangle destination out of bounds read attempt	CVE-2018-4886	Application and Software	2
FILE-OTHER Adobe Acrobat Pro EMF memory corruption attempt	CVE-2018-15951	Application and Software	2
FILE-OTHER Adobe Acrobat Pro EMF out of bounds read attempt	CVE-2018-4986	Application and Software	2
FILE-OTHER Adobe Acrobat Pro EMF out of bounds write attempt	CVE-2018-4895	Application and Software	1
FILE-OTHER Adobe Acrobat Pro EMF use-after-free attempt	CVE-2018-12796	Application and Software	1
FILE-OTHER Adobe Acrobat Pro PDX malformed index out of bounds memory read attempt	CVE-2018-4984	Application and Software	1
FILE-OTHER Adobe Acrobat Pro TIFF embedded XPS file out of bounds read attempt	CVE-2018-16012	Application and Software	2
FILE-OTHER Adobe Acrobat Pro U3D CVE-2018-15952 IFF Out Of Bounds Read	CVE-2018-15952	Application and Software	2
FILE-OTHER Adobe Acrobat Pro XPS ODTTF	CVE-2018-16028	Application and Software	2

out-of-bounds read attempt			
FILE-OTHER Adobe Acrobat Pro XPS ODTTF out-of-bounds read attempt	CVE-2018-19712	Application and Software	2
FILE-OTHER Adobe Acrobat Pro XPS TTF out-of-bounds read attempt	CVE-2018-16001	Application and Software	2
FILE-OTHER Adobe Acrobat Pro XPS file font-load out-of-bounds read attempt	CVE-2018-19711	Application and Software	2
FILE-OTHER Adobe Acrobat Pro XPS file image-load out-of-bounds read attempt	CVE-2018-19704	Application and Software	2
FILE-OTHER Adobe Acrobat Pro XPS file malformed Source attribute buffer overflow attempt	CVE-2018-4899	Application and Software	1
FILE-OTHER Adobe Acrobat Pro XPS file out-of-bounds read attempt	CVE-2018-19714	Application and Software	2
FILE-OTHER Adobe Acrobat Pro XPS malformed TIFF data out of bounds access attempt	CVE-2018-4907	Application and Software	1
FILE-OTHER Adobe Acrobat Pro XPS out of	CVE-2018-4893	Application and Software	1

bounds read attempt			
FILE-OTHER Adobe Acrobat Pro embedded JPEG out of bounds read attempt	CVE-2018-4889	Application and Software	1
FILE-OTHER Adobe Acrobat Pro embedded TIFF heap overflow attempt	CVE-2018-4904	Application and Software	2
FILE-OTHER Adobe Acrobat Pro malformed EMF EmfPlustDrawImagePoints out of bounds read attempt	CVE-2018-4906	Application and Software	2
FILE-OTHER Adobe Acrobat Pro malformed EMF comment memory corruption attempt	CVE-2018-12763	Application and Software	3
FILE-OTHER Adobe Acrobat Pro nested IFD out of bounds read attempt	CVE-2018-4897	Application and Software	1
FILE-OTHER Adobe Acrobat Pro out of bounds read attempt	CVE-2018-15985	Application and Software	2
FILE-OTHER Adobe Acrobat Pro out of bounds read attempt	CVE-2018-15989	Application and Software	2
FILE-OTHER Adobe Acrobat Pro out of bounds read attempt	CVE-2018-16013	Application and Software	2
FILE-OTHER Adobe	CVE-2018-	Application	2

Acrobat Pro out of bounds read attempt	16035	and Software	
FILE-OTHER Adobe Acrobat Pro out of bounds read attempt	CVE-2018-4894	Application and Software	1
FILE-OTHER Adobe Acrobat Pro out-of-bounds read attempt	CVE-2018-4912	Application and Software	2
FILE-OTHER Adobe Acrobat Pro path element out of bounds memory access attempt	CVE-2018-4898	Application and Software	1
FILE-OTHER Adobe Acrobat Pro tiff parser out of bounds read attempt	CVE-2018-19705	Application and Software	2
FILE-OTHER Adobe Acrobat Pro tiff parser out of bounds read attempt	CVE-2018-5016	Application and Software	2
FILE-OTHER Adobe Acrobat Professional EMF JPEG APP13 malformed record crash attempt	CVE-2018-4951	Application and Software	2
FILE-OTHER Adobe Acrobat Reader CVE-2018-12775 Out Of Bounds	CVE-2018-12775	Application and Software	2
FILE-OTHER Adobe Acrobat Reader CVE-2018-12777 Out of Bounds Read Access	CVE-2018-12777	Application and Software	2

FILE-OTHER Adobe Acrobat Reader CVE-2018-12779 Out of Bounds Read Access	CVE-2018-12779	Application and Software	2
FILE-OTHER Adobe Acrobat Reader CVE-2018-12780 Out of Bounds Read Access	CVE-2018-12780	Application and Software	2
FILE-OTHER Adobe Acrobat Reader CVE-2018-12781 Out of Bounds Read Access	CVE-2018-12781	Application and Software	2
FILE-OTHER Adobe Acrobat Reader CVE-2018-12786 Out of Bounds Read	CVE-2018-12786	Application and Software	2
FILE-OTHER Adobe Acrobat Reader CVE-2018-12788 Heap Overflow	CVE-2018-12788	Application and Software	2
FILE-OTHER Adobe Acrobat Reader CVE-2018-12791 Use After Free	CVE-2018-12791	Application and Software	2
FILE-OTHER Adobe Acrobat Reader CVE-2018-12792 Use After Free	CVE-2018-12792	Application and Software	2
FILE-OTHER Adobe Acrobat Reader CVE-2018-12793 Type Confusion	CVE-2018-12793	Application and Software	2
FILE-OTHER Adobe Acrobat Reader CVE-	CVE-2018-12835	Application and Software	2

2018-12835 Out Of Bounds Write			
FILE-OTHER Adobe Acrobat Reader CVE-2019-7116 PostScript Out Of Bounds Read	CVE-2019-7116	Application and Software	2
FILE-OTHER Adobe Acrobat Reader CVE-2019-7125 Arbitrary Code Execution	CVE-2019-7125	Application and Software	2
FILE-OTHER Adobe Acrobat Reader JP2 CVE-2018-4990 Double Free Code Execution	CVE-2018-4990	Application and Software	2
FILE-OTHER Adobe Acrobat and Reader JPEG2000 Parsing Out of Bounds Read	CVE-2019-7794	Application and Software	2
FILE-OTHER Adobe Acrobat and Reader JPEG2000 Parsing Out of Bounds Read	CVE-2019-7794	Application and Software	4
FILE-OTHER Adobe Acrobat malformed font file use after free attempt	CVE-2019-7072	Application and Software	2
FILE-OTHER Adobe Acrobat out of bounds read attempt	CVE-2019-7049	Application and Software	2
FILE-OTHER Adobe Acrobat out-of-bounds read attempt	CVE-2019-7071	Application and Software	2
FILE-OTHER Adobe	CVE-2019-	Application	2

Acrobat out-of-bounds read attempt	7122	and Software	
FILE-OTHER Adobe Acrobat out-of-bounds read attempt	CVE-2019-7127	Application and Software	2
FILE-OTHER Adobe Acrobat out-of-bounds read attempt	CVE-2019-7143	Application and Software	2
FILE-OTHER Adobe Acrobat pro CVE-2018-4908 Out Of Bounds Read Attempt	CVE-2018-4908	Application and Software	2
FILE-OTHER Adobe Acrobat pro CVE-2018-4908 Out Of Bounds Read Attempt	CVE-2018-4908	Application and Software	4
FILE-OTHER Adobe Acrobat pro CVE-2018-4914 Out Of Bounds Read Attempt	CVE-2018-4914	Application and Software	4
FILE-OTHER Adobe Acrobat pro CVE-2018-4914 Out Of Bounds Read Attempt	CVE-2018-4914	Application and Software	2
FILE-OTHER Adobe Acrobat type confusion attempt	CVE-2019-7069	Application and Software	2
FILE-OTHER Adobe Acrobat type confusion attempt	CVE-2019-7128	Application and Software	2
FILE-OTHER Adobe DNG Software Development Kit ReadUncompressed	CVE--2020-9590	Application and Software	1

CVE-2020-9590 Heap-based Buffer Overflow			
FILE-OTHER Adobe DNG Software Development Kit ReadUncompressed CVE-2020-9590 Heap-based Buffer Overflow	CVE--2020-9590	Application and Software	2
FILE-OTHER Adobe Flah Player CVE-2019-7096 GIF Use After Free	CVE-2019-7096	Application and Software	2
FILE-OTHER Adobe Flash Player h264 decoder heap overflow attempt	CVE-2017-2984	Application and Software	1
FILE-OTHER Adobe InDesign Unsafe Hyperlink Processing Remote Code Execution	CVE-2019-7107	Application and Software	2
FILE-OTHER Adobe InDesign Unsafe Hyperlink Processing Remote Code Execution	CVE-2019-7107	Application and Software	4
FILE-OTHER Adobe Professional EMF embedded image heap overflow attempt	CVE-2018-4982	Application and Software	1
FILE-OTHER Adobe Professional EMF file TIFF image size memory corruption attempt	CVE-2017-11261	Application and Software	2
FILE-OTHER Adobe Professional EMF polygon heap buffer overflow attempt	CVE-2017-11241	Application and Software	2

FILE-OTHER Adobe Professional JPEG APP1 memory corruption attempt	CVE-2017-11246	Application and Software	3
FILE-OTHER Adobe Reader CVE-2018-15937 Out Of Bounds Write	CVE-2018-15937	Application and Software	2
FILE-OTHER Adobe Reader CVE-2018-15938 Out Of Bounds Write	CVE-2018-15938	Application and Software	2
FILE-OTHER Adobe Reader CVE-2018-15994 Use After Free	CVE-2018-15994	Application and Software	2
FILE-OTHER Adobe Reader CVE-2018-15997 Information Disclosure	CVE-2018-15997	Application and Software	2
FILE-OTHER Adobe Reader CVE-2018-16008 Use After Free	CVE-2018-16008	Application and Software	2
FILE-OTHER Adobe Reader CVE-2018-16026 Use After Free	CVE-2018-16026	Application and Software	2
FILE-OTHER Adobe Reader CVE-2019-7145 Out Of Bounds Read	CVE-2019-7145	Application and Software	2
FILE-OTHER Adobe Reader CVE-2019-7803 Out Of Bounds Read	CVE-2019-7803	Application and Software	2
FILE-OTHER Adobe Reader CVE-2019-7818 Out Of Bounds Read	CVE-2019-7818	Application and Software	2

FILE-OTHER Adobe Reader CVE-2019-7821 Use After Free	CVE-2019-7821	Application and Software	2
FILE-OTHER Adobe Reader CVE-2019-7828 Heap Overflow	CVE-2019-7828	Application and Software	2
FILE-OTHER Adobe Reader CVE-2019-7829 Out Of Bounds Read	CVE-2019-7829	Application and Software	2
FILE-OTHER Adobe Reader CVE-2019-8019 Type Confusion	CVE-2019-8019	Application and Software	2
FILE-OTHER Adobe Reader CVE-2019-8095 Out Of Bounds Read	CVE-2019-8095	Application and Software	2
FILE-OTHER Adobe Reader CVE-2019-8098 Out Of Bounds Read	CVE-2019-8098	Application and Software	2
FILE-OTHER Adobe Reader EMF CVE-2018-15990 Remote Code Execution	CVE-2018-15990	Application and Software	2
FILE-OTHER Adobe Reader EMF CVE-2018-16006 Use After Free	CVE-2018-16006	Application and Software	2
FILE-OTHER Adobe Reader EMF CVE-2018-16014 Use After Free	CVE-2018-16014	Application and Software	2
FILE-OTHER Adobe Reader EMF CVE-2018-16016 Out Of Bounds Write	CVE-2018-16016	Application and Software	2

FILE-OTHER Adobe Reader EMF CVE-2018-16019 Out Of Bounds	CVE-2018-16019	Application and Software	2
FILE-OTHER Adobe Reader EMF CVE-2018-16021 Heap Overflow	CVE-2018-16021	Application and Software	2
FILE-OTHER Adobe Reader XPS CVE-2018-16015 Out Of Bounds	CVE-2018-16015	Application and Software	2
FILE-OTHER Adobe Reader XPS CVE-2018-19703 Out Of Bounds	CVE-2018-19703	Application and Software	2
FILE-OTHER Adobe.Acrobat CVE-2018-16002 Out of Bounds Read	CVE-2018-16002	Application and Software	2
FILE-OTHER Apple QuickTime PSD File Parsing CVE-2016-1769 Memory Corruption	CVE-2016-1769	Application and Software	2
FILE-OTHER Apple Quicktime TeXML Transform attribute overflow attempt	CVE-2012-0663	Application and Software	1
FILE-OTHER Apple Quicktime TeXML sampleData attribute overflow attempt	CVE-2012-0663	Application and Software	1
FILE-OTHER Apple Safari WebKit HTMLFrameElementBase isURLAllowed Subframe exploit attempt	CVE-2019-8762	Browsers	1

FILE-OTHER Bluezone Desktop buffer overflow attempt		Application and Software	1
FILE-OTHER Cisco WebEx Recording Player memory corruption attempt	CVE-2018-0264	Application and Software	1
FILE-OTHER Cisco WebEx Recording Player memory corruption attempt	CVE-2018-0264	Application and Software	2
FILE-OTHER Cisco Webex Network Recording Player out of bounds write attempt	CVE-2020-3573	Application and Software	3
FILE-OTHER EMF EMR_EXTTEXTOUTW record memory corruption attempt		Application and Software	1
FILE-OTHER EMF EmrText object out of bounds read attempt	CVE-2018-4883	Application and Software	1
FILE-OTHER EMF embedded image out of bound read attempt	CVE-2018-4884	Application and Software	1
FILE-OTHER Everest Software PeakHMI malicious .bsu file buffer overflow attempt		Application and Software	1
FILE-OTHER Flexense DiskPulse Client Import Stack Buffer Overflow I		Application and Software	2
FILE-OTHER Flexense		Application	2

DiskPulse Client Import Stack Buffer Overflow II		and Software	
FILE-OTHER FreeBSD bspatch utility remote code execution attempt CVE-2014-9862	CVE-2014-9862	Application and Software	1
FILE-OTHER GNU Libextractor CVE-2018-16430 ZIP File Comment Out-of-Bounds Read	CVE-2018-16430	Application and Software	2
FILE-OTHER GNU Libextractor CVE-2018-16430 ZIP File Comment Out-of-Bounds Read	CVE-2018-16430	Application and Software	4
FILE-OTHER Ghostscript eqproc type confusion attempt	CVE-2017-8291	Application and Software	2
FILE-OTHER Ghostscript rsdparams type confusion attempt	CVE-2017-8291	Application and Software	2
FILE-OTHER GitLab CVE-2018-14364 Arbitrary File Write	CVE-2018-14364	Application and Software	2
FILE-OTHER Google Golang Get Remote Command Execution	CVE-2018-16873	Application and Software	2
FILE-OTHER Google Golang Get Remote Command Execution	CVE-2018-16873	Application and Software	4
FILE-OTHER Hangul Word Processor type confusion attempt	CVE-2015-6585	Application and Software	2

FILE-OTHER IBM Informix Dynamic Server SET ENVIRONMENT Stack Buffer Overflow CVE-2011-1033	CVE-2011-1033	Application and Software	2
FILE-OTHER IBM Installation Manager iim URI Handling Code Execution		Application and Software	1
FILE-OTHER IBM Installation Manager iim uri code execution attempt	CVE-2009-3518	Application and Software	1
FILE-OTHER KeyView SDK WordPerfect parsing stack buffer overflow attempt		Application and Software	1
FILE-OTHER Lattice Semiconductor ispXCF version attribute overflow attempt		Application and Software	1
FILE-OTHER Maple Maplet File Creation and Command Execution attempt		Application and Software	1
FILE-OTHER Microsoft .NET API XPS file parsing CVE-2020-0605 remote code execution attempt	CVE-2020-0605	Application and Software	2
FILE-OTHER Microsoft Graphics CVE-2017-11763 Remote Code Execution Attempt	CVE-2017-11763	Application and Software	2

FILE-OTHER Microsoft Graphics remote code execution attempt	CVE-2018-8344	Application and Software	2
FILE-OTHER Microsoft Internet Explorer CVE-2012-1524 Attribute Remove Remote Code Execution	CVE-2012-1524	Application and Software	2
FILE-OTHER Microsoft Internet Explorer CVE-2016-7272 Malformed Ico Integer Overflow Attempt	CVE-2016-7272	Application and Software	2
FILE-OTHER Microsoft Jet 4.0 CVE-2016-0250 Access Violation Vulnerability	CVE-2016-0250	Application and Software	1
FILE-OTHER Microsoft Office OLE DLL side load attempt	CVE-2016-7275	Application and Software	2
FILE-OTHER Microsoft Outlook CVE-2019-1199 Use-After-Free Vulnerability	CVE-2019-1199	Application and Software	2
FILE-OTHER Microsoft Windows ATMFD font driver malformed OTF file out-of-bounds memory access attempt	CVE-2017-0192	Application and Software	3
FILE-OTHER Microsoft Windows Address Book Contact file integer overflow attempt	CVE-2020-1410	Application and Software	1
FILE-OTHER Microsoft	CVE-2016-	Application	2

Windows BLF file local privilege escalation attempt	3332	and Software	
FILE-OTHER Microsoft Windows CVE-2013-3128 OpenType Font File Remote Code Execution II	CVE-2013-3128	Application and Software	2
FILE-OTHER Microsoft Windows CVE-2016-7256 OTF Parsing Memory Corruption	CVE-2016-7256	Application and Software	1
FILE-OTHER Microsoft Windows CVE-2016-7274 GDI32.dll cmap numUVSMappings overflow attempt vulnerabilty	CVE-2016-7274	Application and Software	1
FILE-OTHER Microsoft Windows CVE-2018-1013 malformed TTF integer overflow attempt	CVE-2018-1013	Application and Software	2
FILE-OTHER Microsoft Windows Defender CVE-2018-0986 Malformed RAR Memory Corruption Attempt	CVE-2018-0986	Application and Software	1
FILE-OTHER Microsoft Windows Defender malformed RAR memory corruption attempt	CVE-2018-0986	Application and Software	2
FILE-OTHER Microsoft Windows Device Guard bypass via compiled	CVE-2017-8625	Application and Software	2

help file attempt			
FILE-OTHER Microsoft Windows Help Workshop CNT Help contents buffer overflow attempt		Application and Software	1
FILE-OTHER Microsoft Windows Malformed .themepack Theme API Remote Code Execution	CVE-2018-8413	Application and Software	2
FILE-OTHER Microsoft Windows OTF cmap table parsing integer overflow attempt	CVE-2016-7210	Application and Software	3
FILE-OTHER Microsoft Windows OTF parsing memory corruption attempt	CVE-2016-7256	Application and Software	1
FILE-OTHER Microsoft Windows OTF parsing memory corruption attempt	CVE-2016-7256	Application and Software	2
FILE-OTHER Microsoft Windows True Type Font integer overflow attempt	CVE-2015-0059	Application and Software	3
FILE-OTHER Microsoft Windows VBScript Engine VbsErase Memory Corruption	CVE-2019-0667	Application and Software	2
FILE-OTHER Microsoft Windows Vista Feed Headlines Gagdet code	CVE-2007-3033	Application and Software	3

execution attempt			
FILE-OTHER Microsoft Windows malformed TrueType file RCVT out of bounds read attempt	CVE-2016-3209	Application and Software	3
FILE-OTHER Multiple products XML Import Command buffer overflow attempt	CVE-2017-7310	Application and Software	2
FILE-OTHER Oracle CVE-2018-3147 Outside In Excel GelFrame OfficeArtRecLen Out-of-bounds Read	CVE-2018-3147	Application and Software	2
FILE-OTHER Oracle Java Applet Rhino Script Engine Policy CVE-2011-3544 Bypass		Application and Software	2
FILE-OTHER Oracle Java Arbitrary File Deletion 1	CVE- CVE-2019-2449	Application and Software	3
FILE-OTHER Oracle Java Arbitrary File Deletion 2	CVE- CVE-2019-2449	Application and Software	3
FILE-OTHER Oracle Java Arbitrary File Deletion 3	CVE- CVE-2019-2449	Application and Software	3
FILE-OTHER Oracle Java Arbitrary File Deletion 4	CVE-2019-2449	Application and Software	3
FILE-OTHER Oracle Java Runtime Environment ShortComponentRaster.verify CVE-2013-2472 Memory Corruption		Other Web Server	2
FILE-OTHER Oracle Java	CVE-2013-	Application	1

SE CVE-2013-5907 GSUB ReqFeatureIndex Buffer Overflow Vulnerability	5907	and Software	
FILE-OTHER Power Software PowerISO stack buffer overflow attempt	CVE-2017-2817	Application and Software	2
FILE-OTHER Python lib wave.py wav zero channel denial of service attempt	CVE-2017-18207	Application and Software	1
FILE-OTHER TAR file directory traversal attempt	CVE-2020-3238	Application and Software	2
FILE-OTHER Ubisoft Heroes of Might and Magic III .h3m map file buffer overflow attempt		Application and Software	1
FILE-OTHER VMware Fusion Guest VM Remote Code Execution	CVE-2019-5514	Application and Software	2
FILE-OTHER WECON LeviStudioU HFT File Parsing CVE-2020-16243 Stack Buffer Overflow	CVE-2020-16243	Application and Software	5
FILE-PDF ADOBE ActiveX Browser Plugin client side request injection attempt	CVE-2018-4995	Application and Software	2
FILE-PDF Acrobat Reader CVE-2018-12754 Information Disclosure Vulnerability	CVE-2018-12754	Application and Software	2

FILE-PDF Acrobat Reader CVE-2018-12754 Information Disclosure Vulnerability	CVE-2018-12754	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-12756 Information Disclosure Vulnerability	CVE-2018-12756	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-12756 Information Disclosure Vulnerability	CVE-2018-12756	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-12757 Information Disclosure Vulnerability	CVE-2018-12757	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-12757 Information Disclosure Vulnerability	CVE-2018-12757	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-12758 Information Disclosure Vulnerability	CVE-2018-12758	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-12758 Information Disclosure Vulnerability	CVE-2018-12758	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-12760 Information Disclosure Vulnerability	CVE-2018-12760	Application and Software	2
FILE-PDF Acrobat Reader CVE-2018-12760	CVE-2018-12760	Application and Software	1

Information Disclosure Vulnerability			
FILE-PDF Acrobat Reader CVE-2018-12761 Information Disclosure Vulnerability	CVE-2018-12761	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-12764 Information Disclosure Vulnerability	CVE-2018-12764	Application and Software	2
FILE-PDF Acrobat Reader CVE-2018-12764 Information Disclosure Vulnerability	CVE-2018-12764	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-12765 Information Disclosure Vulnerability	CVE-2018-12765	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-12765 Information Disclosure Vulnerability	CVE-2018-12765	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-12766 Information Disclosure Vulnerability	CVE-2018-12766	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-12766 Information Disclosure Vulnerability	CVE-2018-12766	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-12767 Information Disclosure Vulnerability	CVE-2018-12767	Application and Software	2

FILE-PDF Acrobat Reader CVE-2018-12767 Information Disclosure Vulnerability	CVE-2018-12767	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-12768 Information Disclosure Vulnerability	CVE-2018-12768	Application and Software	2
FILE-PDF Acrobat Reader CVE-2018-12768 Information Disclosure Vulnerability	CVE-2018-12768	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-12774 Information Disclosure Vulnerability	CVE-2018-12774	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-12774 Information Disclosure Vulnerability	CVE-2018-12774	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-15925 Information Disclosure Vulnerability	CVE-2018-15925	Application and Software	2
FILE-PDF Acrobat Reader CVE-2018-5050 Information Disclosure Vulnerability	CVE-2018-5050	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-5050 Information Disclosure Vulnerability	CVE-2018-5050	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-5054	CVE-2018-5054	Application and Software	1

Information Disclosure Vulnerability			
FILE-PDF Acrobat Reader CVE-2018-5054 Information Disclosure Vulnerability	CVE-2018-5054	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-5056 Information Disclosure Vulnerability	CVE-2018-5056	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-5056 Information Disclosure Vulnerability	CVE-2018-5056	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-5057 Information Disclosure Vulnerability	CVE-2018-5057	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-5057 Information Disclosure Vulnerability	CVE-2018-5057	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-5063 Information Disclosure Vulnerability	CVE-2018-5063	Application and Software	2
FILE-PDF Acrobat Reader CVE-2018-5063 Information Disclosure Vulnerability	CVE-2018-5063	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-5064 Information Disclosure Vulnerability	CVE-2018-5064	Application and Software	1

FILE-PDF Acrobat Reader CVE-2018-5064 Information Disclosure Vulnerability	CVE-2018-5064	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-5065 Information Disclosure Vulnerability	CVE-2018-5065	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-5065 Information Disclosure Vulnerability	CVE-2018-5065	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-5066 Information Disclosure Vulnerability	CVE-2018-5066	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-5066 Information Disclosure Vulnerability	CVE-2018-5066	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-5069 Information Disclosure Vulnerability	CVE-2018-5069	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-5069 Information Disclosure Vulnerability	CVE-2018-5069	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-5070 Information Disclosure Vulnerability	CVE-2018-5070	Application and Software	1
FILE-PDF Acrobat Reader CVE-2018-5070	CVE-2018-5070	Application and Software	1

Information Disclosure Vulnerability			
FILE-PDF Adobe Acrobat FileAttachment use-after-free attempt	CVE-2016-1065	Application and Software	1
FILE-PDF Adobe Acrobat ImageConversion TIFF Heap-based Buffer Overflow	CVE-2017-2966	Application and Software	1
FILE-PDF Adobe Acrobat JavaScript CVE-2009-0927 getIcon Method Buffer Overflow	CVE-2009-0927	Application and Software	2
FILE-PDF Adobe Acrobat PDF calculate tag use-after-free attempt	CVE-2018-19713	Application and Software	2
FILE-PDF Adobe Acrobat Pro zoom caching use after free attempt	CVE-2016-6971	Application and Software	1
FILE-PDF Adobe Acrobat Reader CVE-2009-3953 U3D CLODMeshDeceleration Code Execution Vulnerability	CVE-2009-3953	Application and Software	2
FILE-PDF Adobe Acrobat Reader CVE-2016-1043 XFA FormCalc replace Integer Overflow	CVE-2016-1043	Application and Software	1
FILE-PDF Adobe Acrobat Reader CVE-2016-4205 malformed embeded TTF File Memory Corruption	CVE-2016-4205	Application and Software	2

FILE-PDF Adobe Acrobat Reader CVE-2019-7121 IFF Information Disclosure	CVE-2019-7121	Application and Software	2
FILE-PDF Adobe Acrobat Reader CVE-2020-9697 Information Disclosure Vulnerability	CVE-2020-9697	Application and Software	1
FILE-PDF Adobe Acrobat Reader CVE-2020-9705 Information Disclosure Vulnerability	CVE-2020-9705	Application and Software	1
FILE-PDF Adobe Acrobat Reader CVE-2020-9706 Information Disclosure Vulnerability	CVE-2020-9706	Application and Software	1
FILE-PDF Adobe Acrobat Reader JPEG engine spurious object reference use after free attempt	CVE-2016-1089	Application and Software	1
FILE-PDF Adobe Acrobat Reader JPEG handling memory corruption attempt	CVE-2016-4252	Application and Software	1
FILE-PDF Adobe Acrobat Reader JPEG parsing out of bounds read attempt	CVE-2016-4192	Application and Software	1
FILE-PDF Adobe Acrobat Reader JPEG2000 CVE-2016-6941 Information Disclosure Vulnerability	CVE-2016-6941	Application and Software	1
FILE-PDF Adobe Acrobat Reader JPEG2000	CVE-2016-1078	Application and Software	1

Information Disclosure			
FILE-PDF Adobe Acrobat Reader Out-of-Bounds Information Disclosure	CVE-2019-16456	Application and Software	1
FILE-PDF Adobe Acrobat Reader PDF CVE-2018-4993 NTML Hash Disclosure	CVE-2018-4993	Application and Software	1
FILE-PDF Adobe Acrobat Reader SaveAs use-after-free attempt	CVE-2016-6945	Application and Software	1
FILE-PDF Adobe Acrobat Reader ToolButton CVE-2013-3346 Use After Free	CVE-2013-3346	Application and Software	5
FILE-PDF Adobe Acrobat Reader U3D CLODMeshDeceleration code execution attempt CVE-2014-0523	CVE-2009-3953	Application and Software	2
FILE-PDF Adobe Acrobat Reader U3D CVE-2018-15953 Information Disclosure	CVE-2018-15953	Application and Software	3
FILE-PDF Adobe Acrobat Reader U3D e3_bone object out of bounds memory access attempt	CVE-2016-1116	Application and Software	1
FILE-PDF Adobe Acrobat Reader XFA addInstance use after free attempt	CVE-2016-6953	Application and Software	1
FILE-PDF Adobe Acrobat Reader XFA excelGroup	CVE-2016-6950	Application and Software	1

memory corruption attempt			
FILE-PDF Adobe Acrobat Reader XFA relayoutPageArea memory corruption attempt	CVE-2016-6952	Application and Software	1
FILE-PDF Adobe Acrobat Reader XObject image object use after free attempt	CVE-2016-1075	Application and Software	1
FILE-PDF Adobe Acrobat Reader XSL stylesheet heap overflow attempt	CVE-2017-2949	Application and Software	1
FILE-PDF Adobe Acrobat Reader XSLT substring memory corruption attempt	CVE-2016-6959	Application and Software	1
FILE-PDF Adobe Acrobat Reader duplicate U3D header memory corruption attempt	CVE-2017-11222	Application and Software	1
FILE-PDF Adobe Acrobat Reader embedded TTF name record out of bounds read attempt	CVE-2016-4203	Application and Software	2
FILE-PDF Adobe Acrobat Reader embedded TTF name record out of bounds read attempt	CVE-2016-4203	Application and Software	1
FILE-PDF Adobe Acrobat Reader go-to action NTLM credential disclosure attempt	CVE-2018-4993	Application and Software	2

FILE-PDF Adobe Acrobat Reader invalid PDF JavaScript printSeps extension call attempt	CVE-2010-4091	Application and Software	1
FILE-PDF Adobe Acrobat Reader malformed CFF global subroutine memory corruption attempt	CVE-2017-2941	Application and Software	1
FILE-PDF Adobe Acrobat Reader malformed FlateDecode stream use after free attempt	CVE-2016-1094	Application and Software	1
FILE-PDF Adobe Acrobat Reader malformed embeded TTF file memory corruption attempt	CVE-2016-4201	Application and Software	2
FILE-PDF Adobe Acrobat Reader malformed embeded TTF file memory corruption attempt	CVE-2016-4205	Application and Software	1
FILE-PDF Adobe Acrobat Reader malformed object stream memory corruption attempt	CVE-2016-6948	Application and Software	1
FILE-PDF Adobe Acrobat Reader malformed unicode font name code execution attempt	CVE-2016-6956	Application and Software	1
FILE-PDF Adobe Acrobat XFA engine stack buffer overflow attempt	CVE-2017-2948	Application and Software	1

FILE-PDF Adobe Acrobat and Reader JPEG2000 Out of Bounds Read	CVE-2017-2946	Application and Software	1
FILE-PDF Adobe Acrobat and Reader JPEG2000 Out of Bounds Read	CVE-2017-2946	Application and Software	4
FILE-PDF Adobe Acrobat invalid embedded font memory corruption attempt	CVE-2016-4208	Application and Software	1
FILE-PDF Adobe Acrobat memory corruption vulnerability attempt	CVE-2016-1081	Application and Software	1
FILE-PDF Adobe Flash Player ActionScript setFocus use after free attempt	CVE-2016-4227	Application and Software	1
FILE-PDF Adobe Flash Player ActionScript setFocus use after free attempt	CVE-2016-4227	Application and Software	2
FILE-PDF Adobe Reader AcroForm dictionary object use after free attempt	CVE-2016-1066	Application and Software	1
FILE-PDF Adobe Reader CTJPEGDecoderReadNextTile out of bounds read attempt	CVE-2016-1077	Application and Software	1
FILE-PDF Adobe Reader CVE-2013-5332 Remote Code Execution	CVE-2013-5332	Application and Software	2
FILE-PDF Adobe Reader	CVE-2016-	Application	2

CVE-2016-1077 CTJPEGDecoderReadNextTile out of bounds read	1077	and Software	
FILE-PDF Adobe Reader CVE-2018-12799 Information Disclosure	CVE-2018-12799	Application and Software	2
FILE-PDF Adobe Reader CVE-2018-12803 Information Disclosure	CVE-2018-12803	Application and Software	2
FILE-PDF Adobe Reader CVE-2018-16005 Information Disclosure	CVE-2018-16005	Application and Software	2
FILE-PDF Adobe Reader CVE-2018-16009 Information Disclosure	CVE-2018-16009	Application and Software	2
FILE-PDF Adobe Reader CVE-2018-16045 Privilege Escalation	CVE-2018-16045	Application and Software	2
FILE-PDF Adobe Reader CVE-2018-19701 Information Disclosure	CVE-2018-19701	Application and Software	2
FILE-PDF Adobe Reader CVE-2018-4955 Information Disclosure	CVE-2018-4955	Application and Software	2
FILE-PDF Adobe Reader CVE-2018-4957 Information Disclosure	CVE-2018-4957	Application and Software	2
FILE-PDF Adobe Reader CVE-2018-4960 Information Disclosure	CVE-2018-4960	Application and Software	2
FILE-PDF Adobe Reader	CVE-2018-	Application	2

CVE-2018-4962 Information Disclosure	4962	and Software	
FILE-PDF Adobe Reader CVE-2018-4973 Information Disclosure	CVE-2018-4973	Application and Software	2
FILE-PDF Adobe Reader DC JPEG2000 CVE-2016-7854 Out-of-Bounds Read	CVE-2016-7854	Application and Software	1
FILE-PDF Adobe Reader DC JPEG2000 CVE-2016-7854 Out-of-Bounds Read	CVE-2016-7854	Application and Software	4
FILE-PDF Adobe Reader DisablePermEnforcement JavaScript function use-after-free attempt	CVE-2016-1084	Application and Software	1
FILE-PDF Adobe Reader Information Disclosure	CVE-2018-4967	Application and Software	2
FILE-PDF Adobe Reader JPEG 2000 COD marker use after free attempt	CVE-2016-6955	Application and Software	1
FILE-PDF Adobe Reader JPEG 2000 memory corruption attempt	CVE-2016-1095	Application and Software	1
FILE-PDF Adobe Reader JavaScript API privileged function bypass attempt	CVE-2016-6957	Application and Software	1
FILE-PDF Adobe Reader JavaScript recursive calls memory corruption attempt	CVE-2016-6970	Application and Software	1

FILE-PDF Adobe Reader JavaScript use after free attempt	CVE-2016-6944	Application and Software	1
FILE-PDF Adobe Reader Javascript ANAuthenticateResource use-after-free attempt	CVE-2018-16040	Application and Software	2
FILE-PDF Adobe Reader MakeAccessible plugin heap overflow attempt	CVE-2016-6939	Application and Software	1
FILE-PDF Adobe Reader PDF CVE-2018-16047 Information Disclosure	CVE-2018-16047	Application and Software	2
FILE-PDF Adobe Reader PDF CVE-2019-7089 Information Disclosure	CVE-2019-7089	Application and Software	2
FILE-PDF Adobe Reader PDF defineGetter execMenuItem use after free attempt	CVE-2016-1047	Application and Software	1
FILE-PDF Adobe Reader PDF embedded JPEG memory corruption attempt	CVE-2016-1088	Application and Software	1
FILE-PDF Adobe Reader PDF execMenuItem use after free attempt	CVE-2016-1047	Application and Software	1
FILE-PDF Adobe Reader PDF onEvent execMenuItem use after free attempt	CVE-2016-1056	Application and Software	1
FILE-PDF Adobe Reader PDF setAction	CVE-2016-1051	Application and Software	1

execMenuItem use after free attempt			
FILE-PDF Adobe Reader PDF setPageAction execMenuItem use after free attempt	CVE-2016-1050	Application and Software	1
FILE-PDF Adobe Reader TrueType font file numberofmetrics out of bounds read attempt	CVE-2016-6954	Application and Software	1
FILE-PDF Adobe Reader Universal 3D engine out of bounds memory access violation attempt	CVE-2016-1074	Application and Software	1
FILE-PDF Adobe Reader XFA API preOpen use after free attempt	CVE-2016-1049	Application and Software	1
FILE-PDF Adobe Reader XFA FormInstanceManager use after free attempt	CVE-2016-1045	Application and Software	1
FILE-PDF Adobe Reader XFA exclGroup JavaScript out of bounds memory access attempt	CVE-2016-6942	Application and Software	1
FILE-PDF Adobe Reader XFA form use-after-free attempt	CVE-2016-1046	Application and Software	1
FILE-PDF Adobe Reader XFA javascript out of bound memory corruption attempt	CVE-2016-1072	Application and Software	1

FILE-PDF Adobe Reader XFA javascript use after free attempt	CVE-2016-1073	Application and Software	1
FILE-PDF Adobe Reader XFA prePrint use after free attempt	CVE-2016-1048	Application and Software	1
FILE-PDF Adobe Reader XFA relayoutPageArea JavaScript out of bounds memory access attempt	CVE-2016-6947	Application and Software	1
FILE-PDF Adobe Reader XFA remerge JavaScript use after free attempt	CVE-2016-6988	Application and Software	1
FILE-PDF Adobe Reader XLST parsing engine use after free attempt	CVE-2016-6979	Application and Software	1
FILE-PDF Adobe Reader XML XSL transform exploitation attempt	CVE-2015-5089	Application and Software	1
FILE-PDF Adobe Reader XSLT Transform use after free attempt	CVE-2016-6961	Application and Software	1
FILE-PDF Adobe Reader XSLT Transform use after free attempt	CVE-2016-6962	Application and Software	1
FILE-PDF Adobe Reader XSLT Transform use after free attempt	CVE-2016-6963	Application and Software	1
FILE-PDF Adobe Reader XSLT Transform use after free attempt	CVE-2016-6964	Application and Software	1

FILE-PDF Adobe Reader XSLT Transform use after free attempt	CVE-2016-6965	Application and Software	1
FILE-PDF Adobe Reader and Acrobat CVE-2009-4324 media.newPlayer Code Execution	CVE-2009-4324	Application and Software	2
FILE-PDF Adobe Reader and Acrobat XSLT function-available Buffer Overflow	CVE-2017-2949	Application and Software	2
FILE-PDF Adobe Reader and Acrobat XSLT function-available Buffer Overflow	CVE-2017-2949	Application and Software	4
FILE-PDF Adobe Reader compareDocuments JavaScript function use-after-free attempt	CVE-2016-1085	Application and Software	1
FILE-PDF Adobe Reader corrupt bookmark use after free attempt	CVE-2016-1091	Application and Software	1
FILE-PDF Adobe Reader createAVView JavaScript use-after-free attempt	CVE-2016-1082	Application and Software	1
FILE-PDF Adobe Reader embedded TTF heap overflow attempt	CVE-2016-4204	Application and Software	1
FILE-PDF Adobe Reader embedded font out of bounds memory access attempt	CVE-2016-4207	Application and Software	1
FILE-PDF Adobe Reader	CVE-2016-	Application	1

execAVDialog JavaScript function use-after-free attempt	1083	and Software	
FILE-PDF Adobe Reader malformed CID identity-H font file out of bounds read attempt	CVE-2016-4206	Application and Software	1
FILE-PDF Adobe Reader malformed ICC profile memory corruption attempt	CVE-2016-4191	Application and Software	1
FILE-PDF Adobe Reader malformed JPEG2000 image invalid NumberComponents out of bounds read attempt	CVE-2016-1078	Application and Software	1
FILE-PDF Adobe Reader malformed Universal 3D stream memory corruption attempt	CVE-2016-1037	Application and Software	1
FILE-PDF Adobe Reader out of bounds memory access violation attempt	CVE-2016-1063	Application and Software	1
FILE-PDF Adobe Reader parser object use-after-free attempt	CVE-2016-6949	Application and Software	1
FILE-PDF Adobe Reader setPersistent use after free attempt	CVE-2016-1061	Application and Software	1
FILE-PDF Adobe Reader submitForm read out of bounds attempt	CVE-2016-1064	Application and Software	1

FILE-PDF Adobe Reader trusted JavaScript function security bypass attempt	CVE-2016-1038	Application and Software	1
FILE-PDF Adobe Reader trusted JavaScript function security bypass attempt	CVE-2016-1039	Application and Software	1
FILE-PDF Adobe Reader trusted JavaScript function security bypass attempt	CVE-2016-1040	Application and Software	1
FILE-PDF Adobe Reader trusted JavaScript function security bypass attempt	CVE-2016-1041	Application and Software	1
FILE-PDF Adobe Reader trusted JavaScript function security bypass attempt	CVE-2016-1042	Application and Software	1
FILE-PDF Adobe Reader trusted JavaScript function security bypass attempt	CVE-2016-1044	Application and Software	1
FILE-PDF Sophos Antivirus PDF parsing stack overflow attempt		Application and Software	1
MALWARE-OTHER Malware Worm.Win32.Wcry.A Runtime Detection		Malware Communication	2
MISC Microsoft Windows Encrypted DCERPC request		Misc	5

attempt			
NETBIOS Cisco WebEx WebExService.exe remote code execution attempt	CVE-2019-1674	Application and Software	1
OS-LINUX Corosync Cluster Engine CVE-2018-1084 totemcrypto.c Integer Overflow	CVE-2018-1084	Operating System and Services	1
OS-LINUX Linux Kernel Netfilter iptables-restore Stack-based Buffer Overflow	CVE-2019-11360	Operating System and Services	2
OS-LINUX Linux Kernel USBIP out of bounds write attempt	CVE-2016-3955	Operating System and Services	1
OS-LINUX Linux kernel SCTP invalid chunk length denial of service attempt	CVE-2016-9555	Operating System and Services	1
OS-LINUX Linux kernel madvise race condition attempt	CVE-2016-5195	Operating System and Services	2
OS-LINUX Linux net af_packet.c tpacket version race condition use after free attempt	CVE-2016-8655	Operating System and Services	2
OS-LINUX OS-LINUX x86 Linux overflow attempt ADMv2		Operating System and Services	1
OS-LINUX OS-LINUX x86 Linux overflow attempt		Operating System and	1

		Services	
OS-LINUX Red Hat 389 CVE-2018-1089 Directory Server ns-slapd ldapsearch Buffer Overflow	CVE-2018-1089	Operating System and Services	2
OS-LINUX Red Hat 389 Directory Server CVE-02018-14624 vslapd_log_emergency_error Denial of Service	CVE-2018-14624	Operating System and Services	1
OS-LINUX Red Hat 389 Directory Server CVE-02018-14624 vslapd_log_emergency_error Denial of Service	CVE-2018-14624	Operating System and Services	4
OS-LINUX Red Hat 389 Directory Server CVE-2018-14648 do_search Denial of Service	CVE-2018-14648	Operating System and Services	1
OS-LINUX Red Hat 389 Directory Server TLS CVE-2019-3883 Resource Exhaustion	CVE-2019-3883	Operating System and Services	1
OS-LINUX Red Hat NetworkManager CVE-2018-1111 DHCP Command Injection	CVE-2018-1111	Operating System and Services	2
OS-LINUX Red Hat NetworkManager DHCP Command Injection CVE-2018-1111	CVE-2018-1111	Operating System and Services	1
OS-OTHER Apple QuickTime FPX File Parsing Memory	CVE-2016-1767	Operating System and	3

Corruption Vulnerability I		Services	
OS-OTHER Apple macOS IOHIDeous exploit download attempt		Operating System and Services	2
OS-OTHER Bash CGI nested loops word_lineno denial of service attempt	CVE-2014-7187	Operating System and Services	1
OS-OTHER SolarWinds Orion NPM OrionModuleEngine Remote Code Execution	CVE-2019-8917	Operating System and Services	1
OS-OTHER multiple operating systems DHCP option overflow attempt	CVE-2008-0084	Operating System and Services	1
OS-WINDOWS Microsoft Graphics Device Interface CVE-2019-1010 Information Disclosure	CVE-2019-1010	Operating System and Services	2
OS-WINDOWS Microsoft Graphics Device Interface CVE-2019-1252 Information Disclosure	CVE-2019-1252	Operating System and Services	2
OS-WINDOWS Microsoft Hyperlink Object Library Information Disclosure	CVE-2016-0059	Operating System and Services	4
OS-WINDOWS Microsoft Windows COM Desktop Broker	CVE-2019-0552	Operating System and Services	2

sandbox escape attempt			
OS-WINDOWS Microsoft Windows CVE-2019-1071 Information Disclosure	CVE-2019-1071	Operating System and Services	1
OS-WINDOWS Microsoft Windows CVE-2019-1073 Information Disclosure	CVE-2019-1073	Operating System and Services	2
OS-WINDOWS Microsoft Windows CVE-2019-1108 Information Disclosure	CVE-2019-1108	Operating System and Services	3
OS-WINDOWS Microsoft Windows Common Log File information disclosure attempt	CVE-2019-1219	Operating System and Services	2
OS-WINDOWS Microsoft Windows CoreShellCOMServerRegistrar privilege escalation attempt	CVE-2019-1184	Operating System and Services	1
OS-WINDOWS Microsoft Windows CredSSP MITM Code Execution	CVE-2018-0886	Operating System and Services	2
OS-WINDOWS Microsoft Windows CryptoAPI TLS server certificate public key with explicitly-defined ECC curve parameters attempt	CVE-2020-0601	Operating System and Services	3

OS-WINDOWS Microsoft Windows Data Sharing Service privilege escalation attempt	CVE-2019-0573	Operating System and Services	2
OS-WINDOWS Microsoft Windows GDI CVE-2019-0758 Information Disclosure	CVE-2019-0758	Operating System and Services	2
OS-WINDOWS Microsoft Windows GDI CVE-2019-0882 Information Disclosure	CVE-2019-0882	Operating System and Services	2
OS-WINDOWS Microsoft Windows GDI invalid EMF cbBitsSrc memory disclosure attempt	CVE-2017-0038	Operating System and Services	2
OS-WINDOWS Microsoft Windows Graphics Component CVE-2017-8676 Information Disclosure	CVE-2017-8676	Operating System and Services	2
OS-WINDOWS Microsoft Windows Graphics Device CVE-2018-8424 Interface Information Disclosure	CVE-2018-8424	Operating System and Services	3
OS-WINDOWS Microsoft Windows Graphics Device CVE-2018-8424 Interface Information Disclosure	CVE-2018-8424	Operating System and Services	4
OS-WINDOWS Microsoft Windows	CVE-2003-0907	Operating System and	1

Help Centre escape sequence XSS attempt		Services	
OS-WINDOWS Microsoft Windows JET Database Engine Physical Index Out-of-Bounds Read CVE-2019-0575	CVE-2019-0575	Operating System and Services	2
OS-WINDOWS Microsoft Windows JET Database Engine Physical Index Out-of-Bounds Read CVE-2019-0575	CVE-2019-0575	Operating System and Services	4
OS-WINDOWS Microsoft Windows Kerberos auth downgrade to DES MITM attempt	CVE-2011-0091	Operating System and Services	3
OS-WINDOWS Microsoft Windows Kernel information disclosure attempt	CVE-2019-0844	Operating System and Services	2
OS-WINDOWS Microsoft Windows LSASS Authentication Denial of Service	CVE-2017-0004	Operating System and Services	2
OS-WINDOWS Microsoft Windows NT MiRelocateImage out of bounds read attempt	CVE-2019-1347	Operating System and Services	1
OS-WINDOWS Microsoft Windows NT MiRelocateImage out of bounds read attempt	CVE-2019-1347	Operating System and Services	2

OS-WINDOWS Microsoft Windows NtSetCachedSigningLevel Device Guard bypass attempt	CVE-2019-0732	Operating System and Services	2
OS-WINDOWS Microsoft Windows Ntoskrnl integer overflow privilege escalation attempt	CVE-2016-0070	Operating System and Services	3
OS-WINDOWS Microsoft Windows Remote Desktop Protocol Server Information Disclosure Vulnerability	CVE-2019-1224	Operating System and Services	2
OS-WINDOWS Microsoft Windows SMB srv2.sys information disclosure attempt	CVE-2020-1206	Operating System and Services	1
OS-WINDOWS Microsoft Windows SMBv1 WriteAndX and TransSecondaryRequest TotalDataCount out of bounds write attempt	CVE-2017-0145	Operating System and Services	1
OS-WINDOWS Microsoft Windows SMBv1 identical MID and FID type confusion attempt CVE-2017-0143	CVE-2017-0143	Operating System and Services	2
OS-WINDOWS Microsoft Windows SMBv1 identical MID and FID type confusion	CVE-2017-0143	Operating System and Services	2

attempt			
OS-WINDOWS Microsoft Windows SMBv3 Compression Information Disclosure	CVE-2020-1206	Operating System and Services	1
OS-WINDOWS Microsoft Windows Win32k Information Disclosure Vulnerability	CVE-2019-1469	Operating System and Services	1
OS-WINDOWS Microsoft Windows Win32k kernel information disclosure attempt	CVE-2019-1436	Operating System and Services	1
OS-WINDOWS Microsoft Windows kernel information disclosure attempt	CVE-2019-0840	Operating System and Services	2
OS-WINDOWS Microsoft Windows malformed NTLMv2 authentication message attempt	CVE-2019-1019	Operating System and Services	2
OS-WINDOWS Microsoft Windows operating system win32kfull heap corruption attempt	CVE-2016-3308	Operating System and Services	2
OS-WINDOWS Windows Kernel CVE-2019-0767 Information Disclosure Vulnerability	CVE-2019-0767	Operating System and Services	2
OS-WINDOWS Windows Network File System NLM RPC Message CVE-	CVE-2020-17056	Operating System and	5

2020-17056 Information Disclosure		Services	
OS-WINDOWS Windows Uniscribe CVE-2017-0014 Remote Code Execution	CVE-2017-0014	Operating System and Services	1
PROTOCOL-DNS Cisco ASA and FTD IPv6 DNS request stack buffer overflow attempt	CVE-2020-3191	DNS	1
PROTOCOL-DNS Cisco IOS XE Umbrella Connector denial of service attempt	CVE-2020-3510	DNS	1
PROTOCOL-DNS ISC BIND TSIG Validation Denial of Service	CVE-2020-8617	DNS	1
PROTOCOL-DNS Oracle Secure Backup observice.exe dns response overflow attempt	CVE-2010-0072	DNS	1
PROTOCOL-OTHER FreeRDP RSA modulus length integer underflow attempt	CVE-2017-2836	Operating System and Services	2
PROTOCOL-OTHER Quagga BGP Daemon CVE-2018-5379 bgp_update_receive Double Free I	CVE-2018-5379	Operating System and Services	1
PROTOCOL-OTHER Quagga BGP Daemon CVE-2018-5379 bgp_update_receive	CVE-2018-5379	Operating System and Services	1

Double Free II			
PROTOCOL-OTHER VMware vCenter Server Directory Service CVE-2020-3952 Authentication Bypass	CVE-2020-3952	Other Web Server	3
PROTOCOL-RPC IBM Informix Dynamic Server librpc.dll buffer overflow attempt	CVE-2009-2753	Operating System and Services	1
PROTOCOL-RPC Linux kernel NFSv2 malformed WRITE arbitrary memory read attempt	CVE-2017-7895	Operating System and Services	1
PROTOCOL-RPC Linux kernel NFSv3 malformed WRITE arbitrary memory read attempt	CVE-2017-7895	Operating System and Services	1
PROTOCOL-RPC Oracle Solaris sadmind TCP array size buffer overflow attempt	CVE-2008-3869	Operating System and Services	1
PROTOCOL-RPC Oracle Solaris sadmind TCP data length integer overflow attempt	CVE-2008-3870	Operating System and Services	1
PROTOCOL-RPC Oracle Solaris sadmind UDP array size buffer overflow attempt	CVE-2008-3869	Operating System and Services	1
PROTOCOL-RPC Oracle Solaris sadmind UDP data length integer	CVE-2008-3870	Operating System and	1

overflow attempt		Services	
PROTOCOL-RPC xdrDecodeString caller_name stack overflow attempt	CVE-2010-4227	Operating System and Services	1
PROTOCOL-SERVICES LibVNCClient CVE-2016-9941 FramebufferUpdate Heap Buffer Overflow I	CVE-2016-9941	Operating System and Services	3
PROTOCOL-SERVICES LibVNCClient CVE-2016-9941 FramebufferUpdate Heap Buffer Overflow II	CVE-2016-9941	Operating System and Services	3
PROTOCOL-SNMP Cisco IOS IS-IS SNMP denial of service attempt	CVE-2019-16027	Operating System and Services	2
PROTOCOL-SNMP Cisco Small Business Series Switches SNMP denial of service attempt	CVE-2019-1806	Operating System and Services	1
PROTOCOL-TFTP Cisco Prime Infrastructure swimtemp TFTP Arbitrary File Upload	CVE-2018-15379	FTP	1
PROTOCOL-TFTP HP Intelligent Management Center TFTP Server DATA and ERROR Packets Buffer Overflow		FTP	1
PROTOCOL-TFTP HPE Intelligent Management Center PLAT tftpserver fread Stack Buffer	CVE-2018-7074	FTP	1

Overflow CVE-2018-7074			
PROTOCOL-VOIP Asterisk CVE-2018-1000099 PJSIP Invalid fmtp Media Attribute Denial Of Service	CVE-2018-1000099	VoIP and Instant Messaging	2
PROTOCOL-VOIP Cisco Unified Customer Voice Portal denial of service attempt	CVE-2018-0086	VoIP and Instant Messaging	2
PROTOCOL-VOIP Digium Asterisk Manager Interface initial banner		VoIP and Instant Messaging	4
PROTOCOL-VOIP Digium Asterisk Manager User Shell Command Execution	CVE-2019-18610	VoIP and Instant Messaging	2
SERVER-APACHE (Published Exploit) BEA WebLogic Server Apache Connector HTTP Version String Buffer Overflow	CVE-2008-3257	Apache HTTP Server	1
SERVER-APACHE Apache APR memory corruption attempt	CVE-2003-0245	Apache HTTP Server	3
SERVER-APACHE Apache ActiveMQ CVE-2016-3088 Fileserver MOVE Directory Traversal	CVE-2016-3088	Apache HTTP Server	2
SERVER-APACHE Apache ActiveMQ CVE-2018-8006 Web Console QueueFilter Cross-Site	CVE-2018-8006	Apache HTTP Server	1

Scripting			
SERVER-APACHE Apache ActiveMQ CVE-2018-8006 Web Console QueueFilter Cross-Site Scripting	CVE-2018-8006	Apache HTTP Server	2
SERVER-APACHE Apache ActiveMQ Fileserver File Upload Directory Traversal	CVE-2016-3088	Apache HTTP Server	2
SERVER-APACHE Apache CVE-2018-1306 Pluto PortletV3AnnotatedDemo MultipartPortlet Arbitrary File Upload	CVE-2018-1306	Apache HTTP Server	2
SERVER-APACHE Apache CVE-2018-8007 CouchDB _config Command Execution	CVE-2018-8007	Apache HTTP Server	2
SERVER-APACHE Apache Commons FileUpload Boundary Denial of Service	CVE-2016-3092	Apache HTTP Server	2
SERVER-APACHE Apache Continuum saveInstallation.action Command Injection		Apache HTTP Server	1
SERVER-APACHE Apache CouchDB CVE-2017-12635 JSON Remote Privilege Escalation	CVE-2017-12635	Apache HTTP Server	2
SERVER-APACHE Apache CouchDB JSON Remote Privilege Escalation	CVE-2017-12635	Apache HTTP Server	4

SERVER-APACHE Apache CouchDB _config Command Execution	CVE-2017-12636	Apache HTTP Server	2
SERVER-APACHE Apache Dubbo HttpRemoteInvocation CVE-2019-17564 Insecure Deserialization	CVE-2019-17564	Apache HTTP Server	1
SERVER-APACHE Apache HTTP Server CVE-2016-8740 mod_http2 Module Denial of Service	CVE-2016-8740	Apache HTTP Server	4
SERVER-APACHE Apache HTTP Server mod_http2 Module Denial of Service	CVE-2016-8740	Apache HTTP Server	3
SERVER-APACHE Apache HTTP Server mod_http2 denial of service attempt	CVE-2016-8740	Apache HTTP Server	2
SERVER-APACHE Apache Kylin REST API DiagnosisService CVE-2020-13925 Command Injection	CVE-2020-13925	Apache HTTP Server	2
SERVER-APACHE Apache Kylin REST API migrateCube CVE-2020-1956 Command Injection	CVE-2020-1956	Apache HTTP Server	1
SERVER-APACHE Apache Log4j SocketServer Untrusted Deserialization	CVE-2019-17571	Apache HTTP Server	1

SERVER-APACHE Apache OFBiz XMLRPC CVE-2020-9496 Insecure Deserialization	CVE-2020-9496	Apache HTTP Server	2
SERVER-APACHE Apache OFBiz serviceContext XStream Insecure Deserialization	CVE-2019-0189	Apache HTTP Server	1
SERVER-APACHE Apache OFBiz serviceContext XStream Insecure Deserialization	CVE-2019-0189	Apache HTTP Server	2
SERVER-APACHE Apache Olingo CVE-2019-17554 XML Deserializer External Entity Injection	CVE-2019-17554	Apache HTTP Server	1
SERVER-APACHE Apache Qpid AMPQ denial of service attempt	CVE-2015-0203	Apache HTTP Server	1
SERVER-APACHE Apache Qpid Sequence Set Denial of Service	CVE-2015-0203	Apache HTTP Server	1
SERVER-APACHE Apache Qpid Sequence Set Denial of Service	CVE-2015-0203	Apache HTTP Server	4
SERVER-APACHE Apache Qpid Session.gap Denial of Service	CVE-2015-0203	Apache HTTP Server	1
SERVER-APACHE Apache Qpid Session.gap Denial of Service	CVE-2015-0203	Apache HTTP Server	4
SERVER-APACHE Apache ShardingSphere	CVE-2020-1947	Web Services and	3

SnakeYAML CVE-2020-1947 Insecure Deserialization		Applications	
SERVER-APACHE Apache Solr CVE-2018-8026 ConfigSets XML External Entity Expansion Information Disclosure	CVE-2018-8026	Apache HTTP Server	3
SERVER-APACHE Apache Solr Config API Insecure Deserialization	CVE-2019-0192	Apache HTTP Server	1
SERVER-APACHE Apache Solr Config API Insecure Deserialization	CVE-2019-0192	Apache HTTP Server	2
SERVER-APACHE Apache Solr Config API Insecure Deserialization	CVE-2019-0192	Apache HTTP Server	4
SERVER-APACHE Apache Solr ConfigSets CVE-2018-8010 XML External Entity Expansion Information Disclosure	CVE-2018-8010	Apache HTTP Server	3
SERVER-APACHE Apache Solr Data Import Handler XML External Entity Expansion Information Disclosure 2018-1308	CVE-2018-1308	Apache HTTP Server	1
SERVER-APACHE Apache Solr DataImportHandler Remote Code Execution	CVE-2019-0193	Apache HTTP Server	1
SERVER-APACHE Apache Solr RunExecutableListener	CVE-2017-12629	Apache HTTP Server	2

arbitrary command execution attempt			
SERVER-APACHE Apache Solr Velocity Response Writer CVE-2019-17558 Remote Code Execution		Apache HTTP Server	1
SERVER-APACHE Apache Solr xmlparser XML External Entity Expansion Remote Code Execution	CVE-2017-12629	Apache HTTP Server	2
SERVER-APACHE Apache Solr xmlparser external doctype or entity expansion attempt	CVE-2017-12629	Apache HTTP Server	2
SERVER-APACHE Apache Spark auth-enabled standalone master (CVE-2020-9480) Command Execution	CVE-2020-9480	Apache HTTP Server	1
SERVER-APACHE Apache Spark auth-enabled standalone master (CVE-2020-9480) Command Execution	CVE-2020-9480	Apache HTTP Server	5
SERVER-APACHE Apache Struts 2 ConversionErrorInterceptor OGNL Script Injection	CVE-2012-0391	Apache HTTP Server	1
SERVER-APACHE Apache Struts 2 ParametersInterceptor OGNL Command Execution	CVE-2011-3923	Apache HTTP Server	1

SERVER-APACHE Apache Struts 2 Struts 1 Plugin Remote Code Execution	CVE-2017-9791	Apache HTTP Server	2
SERVER-APACHE Apache Struts CVE-2016-4465 URLValidator Denial of Service I	CVE-2016-4465	Apache HTTP Server	2
SERVER-APACHE Apache Struts OGNL CVE-2019-0230 Remote Code Execution	CVE-2019-0230	Apache HTTP Server	2
SERVER-APACHE Apache Struts REST Plugin DMI Code Execution	CVE-2016-3087	Apache HTTP Server	2
SERVER-APACHE Apache Struts URL and Anchor tag includeParams OGNL Command Execution	CVE-2013-2115	Apache HTTP Server	1
SERVER-APACHE Apache Struts arbitrary OGNL remote code execution attempt	CVE-2013-2135	Apache HTTP Server	1
SERVER-APACHE Apache Struts parameters interceptor remote code execution attempt	CVE-2011-3923	Apache HTTP Server	1
SERVER-APACHE Apache Struts remote code execution attempt - CookieInterceptor	CVE-2012-0392	Apache HTTP Server	1
SERVER-APACHE Apache Struts wildcard matching OGNL remote	CVE-2013-2134	Apache HTTP Server	1

code execution attempt			
SERVER-APACHE Apache Struts xslt.location local file inclusion attempt	CVE-2016-3082	Apache HTTP Server	1
SERVER-APACHE Apache Struts2 CVE-2017-9791 Remote Code Execution II	CVE-2017-9791	Apache HTTP Server	2
SERVER-APACHE Apache Struts2 File Upload CVE-2009-0233 Denial of Service	CVE-2019-0233	Apache HTTP Server	2
SERVER-APACHE Apache Struts2 File Upload CVE-2019-0233 Denial of Service	CVE-2019-0233	Apache HTTP Server	2
SERVER-APACHE Apache Struts2 remote code execution attempt	CVE-2013-2251	Apache HTTP Server	1
SERVER-APACHE Apache Struts2 remote code execution attempt	CVE-2013-2251	Apache HTTP Server	2
SERVER-APACHE Apache Subversion mod_authz_svn COPY MOVE Denial of Service	CVE-2016-2168	Apache HTTP Server	3
SERVER-APACHE Apache Subversion mod_dav_svn Denial of Service	CVE-2018-11803	Apache HTTP Server	1
SERVER-APACHE Apache Subversion mod_dav_svn Integer	CVE-2015-5343	Apache HTTP Server	2

Overflow			
SERVER-APACHE Apache Subversion svn-ssh URL Command Execution	CVE-2017-9800	Apache HTTP Server	1
SERVER-APACHE Apache Tapestry ContextAssetRequestHandler CVE-2020-13953 Information Disclosure	CVE-2020-13953	Apache HTTP Server	3
SERVER-APACHE Apache Tika tika-server Command Injection Vulnerability	CVE-2018-1335	Apache HTTP Server	1
SERVER-APACHE Apache Tomcat AJP Local File Inclusion	CVE-2020-1938	Apache HTTP Server	1
SERVER-APACHE Apache Tomcat CVE-2017-12615 HTTP PUT Windows Remote Code Execution	CVE-2017-12615	Apache HTTP Server	2
SERVER-APACHE Apache Tomcat CVE-2017-12617 HTTP PUT Remote Code Execution	CVE-2017-12617	Apache HTTP Server	2
SERVER-APACHE Apache Tomcat CVE-2018-11784 Default Servlet Open Redirect	CVE-2018-11784	Apache HTTP Server	3
SERVER-APACHE Apache Tomcat CVE-2018-11784 Default Servlet Open Redirect	CVE-2018-11784	Apache HTTP Server	4

SERVER-APACHE Apache Tomcat HTTP PUT CVE-2017-12615 Windows Remote Code Execution	CVE-2017-12615	Apache HTTP Server	2
SERVER-APACHE Apache Tomcat HTTP PUT Remote Code Execution	CVE-2017-12615	Apache HTTP Server	1
SERVER-APACHE Apache Tomcat HTTP2 Connection Window Exhaustion Denial Of Service	CVE-2019-10072	Apache HTTP Server	2
SERVER-APACHE Apache Tomcat HTTP2 h2c Memory Exhaustion	CVE-2020-13934	Apache HTTP Server	1
SERVER-APACHE Apache Tomcat Java JmxRemoteLifecycleListener unauthorized serialized object attempt	CVE-2016-8735	Apache HTTP Server	1
SERVER-APACHE Apache Tomcat WebSocket Infinite Loop CVE-2020-13935 Denial of Service	CVE-2020-13935	Apache HTTP Server	2
SERVER-APACHE Apache Tomcat WebSocket Infinite Loop CVE-2020-13935 Denial of Service	CVE-2020-13935	Apache HTTP Server	5
SERVER-APACHE Apache Traffic Server ESI Plugin Cookie Header Information Disclosure CVE-2018-8040	CVE-2018-8040	Apache HTTP Server	2

SERVER-APACHE Apache httpd CVE-2018-8011 mod_md Null Pointer Dereference	CVE-2018-8011	Apache HTTP Server	2
SERVER-APACHE Apache httpd CVE-2019-0190 mod_ssl TLS Renegotiation Denial of Service		Apache HTTP Server	3
SERVER-APACHE Apache httpd FilesMatch Directive Security Restriction Bypass CVE-2017-15715	CVE-2017-15715	Apache HTTP Server	1
SERVER-APACHE Apache httpd FilesMatch Directive Security Restriction Bypass CVE-2017-15715	CVE-2017-15715	Apache HTTP Server	2
SERVER-APACHE Apache httpd ap_find_token Out of Bounds Read	CVE-2017-7668	Apache HTTP Server	2
SERVER-APACHE Apache httpd mod_cache_socache Denial of Service	CVE-2018-1303	Apache HTTP Server	1
SERVER-APACHE Apache httpd mod_remoteip Buffer Overflow	CVE-2019-10097	Apache HTTP Server	1
SERVER-APACHE Apache mod_session_crypto padding oracle brute force attempt	CVE-2016-0736	Apache HTTP Server	3
SERVER-APACHE BEA	CVE-2008-	Apache HTTP	1

WebLogic Apache Oracle connector Transfer-Encoding buffer overflow attempt	4008	Server	
SERVER-APACHE Oracle WebLogic Apache Connector buffer overflow attempt	CVE-2008-3257	Apache HTTP Server	1
SERVER-APACHE Red5 Server Apache Commons Collections Insecure Deserialization		Apache HTTP Server	1
SERVER-APACHE Red5 Server Apache Commons Collections Insecure Deserialization		Apache HTTP Server	4
SERVER-APACHE httpd mod_mime content-type buffer overflow attempt	CVE-2017-7679	Apache HTTP Server	1
SERVER-IIS Microsoft Windows IIS .NET null character username truncation attempt	CVE-2011-3416	Microsoft IIS web server	2
SERVER-MAIL IBM Domino IMAP Mailbox Name Stack Buffer Overflow	CVE-2017-1274	Other Mail Server	3
SERVER-MAIL IBM Lotus Notes URI handler command execution attempt	CVE-2012-2174	Other Mail Server	3
SERVER-MAIL IBM Lotus Notes WPD attachment handling buffer	CVE-2008-4564	Other Mail Server	1

overflow attempt			
SERVER-MAIL Mail.app AppleSingleDouble command execution attempt	CVE-2016-0395	Other Mail Server	2
SERVER-MAIL Novell iPrint Client CVE-2013-1091 For Windows IPP Response Stack Buffer Overflow	CVE-2013-1091	Other Mail Server	4
SERVER-MAIL Novell iPrint Client ienipp.ocx volatile-date-time Parsing Buffer Overflow	CVE-2009-1569	Other Mail Server	2
SERVER-MSSQL Microsoft SQL RDBMS Engine CVE-2016-7250 UNC Path Injection Privilege Escalation II	CVE-2016-7250	Database Management System	1
SERVER-MSSQL Microsoft SQL RDBMS Engine UNC Path Injection Privilege Escalation (Published Exploit)	CVE-2016-7250	Database Management System	1
SERVER-MYSQL Multiple SQL products privilege escalation attempt	CVE-2016-6662	Database Management System	1
SERVER-ORACLE BEA WebLogic CVE-2014-6321 SSL Handling Denial of Service	CVE-2014-6321	Database Management System	1
SERVER-ORACLE Oracle BEA WebLogic CVE-		Database Management	2

2008-5457 Server Apache Connector Buffer Overflow		System	
SERVER-ORACLE Oracle BEA WebLogic IIS connector JSESSIONID Stack Buffer Overflow	CVE-2008-5457	Database Management System	1
SERVER-ORACLE Oracle Document Capture File Overwrite Buffer Overflow I	CVE-2010-3599	Database Management System	1
SERVER-ORACLE Oracle Fusion Middleware MapViewer FileUploaderServlet fileName Directory Traversal	CVE-2017-3230	Database Management System	1
SERVER-ORACLE Oracle Fusion Middleware MapViewer FileUploaderServlet fileName Directory Traversal	CVE-2017-3230	Database Management System	3
SERVER-ORACLE Oracle GoldenGate CVE-2018-2913 Manager Command Stack Buffer Overflow I	CVE-2018-2913	Database Management System	2
SERVER-ORACLE Oracle GoldenGate CVE-2018-2913 Manager Command Stack Buffer Overflow II	CVE-2018-2913	Database Management System	2
SERVER-ORACLE Oracle GoldenGate Manager CVE-2018-2914	CVE-2018-2914	Database Management	3

Command Report Denial of Service		System	
SERVER-ORACLE Oracle GoldenGate Manager Command Tab Parsing Denial of Service	CVE-2018-2912	Database Management System	1
SERVER-ORACLE Oracle Java Applet2ClassLoader Remote Code Execution	CVE-2010-4452	Database Management System	1
SERVER-ORACLE Oracle Java Runtime Bytecode Verifier Cache Code Execution (Published Exploit)	CVE-2012-1723	Database Management System	1
SERVER-ORACLE Oracle Java Runtime Bytecode Verifier Cache Code Execution (Published Exploit)	CVE-2012-1723	Database Management System	4
SERVER-ORACLE Oracle Java Runtime Environment CVE-2013-2465 storeImageArray Buffer Overflow	CVE-2013-2465	Database Management System	2
SERVER-ORACLE Oracle Java Runtime Environment ShortComponentRaster.verify Memory Corruption (Published Exploit)	CVE-2013-2472	Database Management System	1
SERVER-ORACLE Oracle Java Runtime Environment ShortComponentRaster.	CVE-2013-2472	Database Management System	4

verify Memory Corruption (Published Exploit)			
SERVER-ORACLE Oracle Java Runtime Environment storeImageArray Buffer Overflow (Published Exploit)	CVE-2013-2465	Database Management System	2
SERVER-ORACLE Oracle Java Runtime Environment storeImageArray Buffer Overflow (Published Exploit)	CVE-2013-2465	Database Management System	4
SERVER-ORACLE Oracle Java Runtime Environment storeImageArray Buffer Overflow (Published Exploit)	CVE-2013-2465	Database Management System	2
SERVER-ORACLE Oracle Java Web Start Command Argument Injection Remote Code Execution	CVE-2012-0500	Database Management System	1
SERVER-ORACLE Oracle Java Web Start Command Argument Injection Remote Code Execution	CVE-2012-0500	Database Management System	4
SERVER-ORACLE Oracle Java Web Start Launch Command-Line Injection		Database Management System	1

SERVER-ORACLE Oracle MySQL sql_authentication Integer Overflow	CVE-2017-3599	Database Management System	2
SERVER-ORACLE Oracle Outside CVE-2018-2992 In Excel GelFrame Out-of-bounds Read	CVE-2018-2992	Database Management System	3
SERVER-ORACLE Oracle Outside In JPEG 2000 COD and COC Parameter Heap Buffer Overflow	CVE-2011-4516	Database Management System	4
SERVER-ORACLE Oracle Secure Backup NDMP CONECT_CLIENT_AUTH Command Buffer Overflow	CVE-2008-5444	Database Management System	1
SERVER-ORACLE Oracle Secure Backup exec_qr command injection attempt	CVE-2008-5448	Database Management System	1
SERVER-ORACLE Oracle Solaris RPC CVE-2017-3623 Heap Buffer Overflow	CVE-2017-3623	Database Management System	2
SERVER-ORACLE Oracle Tuxedo Jolt Protocol CVE-2017-10278 Heap Buffer Overflow	CVE-2017-10278	Database Management System	3
SERVER-ORACLE Oracle Web Cache CVE-2018-0967 Unspecified Client Request Handling log	CVE-2004-0385	Database Management System	2

SERVER-ORACLE Oracle WebLogic CVE-2018-2616 Remote Diagnosis Assistant rda_tfa_hrs Command Injection	CVE-2018-2616	Database Management System	2
SERVER-ORACLE Oracle WebLogic Server AbstractPlatformTransactionManager Insecure Deserialization CVE-2018-3191	CVE-2018-3191	Database Management System	2
SERVER-ORACLE Oracle WebLogic Server CVE-2018-2894 Web Service Config Arbitrary File Upload	CVE-2018-2894	Database Management System	3
SERVER-ORACLE Oracle WebLogic Server DeploymentServiceServlet Insecure Deserialization	CVE-2018-3252	Database Management System	2
SERVER-ORACLE Oracle WebLogic Server FileDistributionServlet Information Disclosure	CVE-2019-2615	Database Management System	2
SERVER-ORACLE Oracle WebLogic Server Node Manager Command Execution		Database Management System	1
SERVER-ORACLE Oracle WebLogic Server RemoteObject Insecure Deserialization	CVE-2018-3245	Database Management System	1
SERVER-ORACLE Oracle WebLogic Server	CVE-2017-3248	Database Management	2

UnicastRef Insecure Deserialization		System	
SERVER-ORACLE Oracle WebLogic Server UnicastRef Insecure Deserialization	CVE-2017-3248	Database Management System	4
SERVER-ORACLE Oracle WebLogic Server remote command execution attempt	CVE-2017-10271	Database Management System	2
SERVER-ORACLE Oracle WebLogic Server remote command execution attempt	CVE-2017-10271	Web Services and Applications	1
SERVER-ORACLE Oracle Weblogic CVE-2020-2551 Insecure Deserialization	CVE-2020-2551	Other Web Server	1
SERVER-ORACLE Oracle Weblogic LimitFilter Insecure Deserialization	CVE-2020-2555	Other Web Server	1
SERVER-ORACLE Oracle iPlanet Web Server unauthenticated information disclosure attempt	CVE-2020-9315	Other Web Server	1
SERVER-ORACLE Oracle iPlanet admin panel image injection attempt	CVE-2020-9314	Other Web Server	1
SERVER-ORACLE Secure Backup administration server login.php cookies command injection attempt	CVE-2008-4006	Database Management System	1

SERVER-ORACLE Secure Backup common.php variable based command injection attempt	CVE-2008-4006	Database Management System	1
SERVER-ORACLE Secure Backup msgid 0x901 username field overflow attempt	CVE-2008-5444	Database Management System	1
SERVER-ORACLE WebLogic Server Node Manager arbitrary command execution attempt	CVE-2010-0073	Database Management System	1
SERVER-ORACLE auth_sesskey buffer overflow attempt	CVE-2009-1979	Database Management System	1
SERVER-OTHER Active Directory LDAP addRequest crafted dnsRecord information leak attempt	CVE-2020-0856	Other Web Server	2
SERVER-OTHER Adobe ColdFusion CVE-2017-11284 RMI Registry Insecure Deserialization	CVE-2017-11284	Other Web Server	1
SERVER-OTHER Adobe ColdFusion CVE-2017-11284 RMI Registry Insecure Deserialization	CVE-2017-11284	Other Web Server	4
SERVER-OTHER Adobe ColdFusion arbitrary file upload attempt CVE-2019-7816	CVE-2019-7816	Application and Software	2

SERVER-OTHER Advantech WebAccess Client bwswfcfg Stack-based Buffer Overflow	CVE-2018-17910	Other Web Server	2
SERVER-OTHER Advantech WebAccess Node spchapi and tv_enua Stack Buffer Overflow		Other Web Server	2
SERVER-OTHER Advantech WebAccess webvrpcs service arbitrary pointer dereference attempt	CVE-2017-16728	Other Web Server	2
SERVER-OTHER Aerospike Database Server Fabric denial of service attempt	CVE-2016-9049	Other Web Server	2
SERVER-OTHER Aerospike Database Server si_prop stack buffer overflow attempt	CVE-2016-9054	Other Web Server	2
SERVER-OTHER Apache OFBiz XMLRPC deserialization attempt	CVE-2020-9496	Other Web Server	2
SERVER-OTHER Apache mod_auth_digest out of bounds read attempt	CVE-2017-9788	Other Web Server	1
SERVER-OTHER BigAnt Document Service DDNF request stack buffer overflow attempt		Other Web Server	1
SERVER-OTHER CA ARCserve Backup for	CVE-2008-3175	Other Web Server	1

Laptops and Desktops LGServer Handshake Buffer Overflow			
SERVER-OTHER CA ARCserve Backup for Laptops and Desktops LGServer handshake buffer overflow attempt	CVE-2008-3175	Other Web Server	1
SERVER-OTHER CA XOsoft Multiple Products xosoapapi.asmx Buffer Overflow	CVE-2010-1223	Other Web Server	1
SERVER-OTHER CA XOsoft Multiple Products xosoapapi.asmx Buffer Overflow	CVE-2010-1223	Other Web Server	4
SERVER-OTHER Cesanta Mongoose parse_mqtt Out of Bounds Read	CVE-2019-12951	Other Web Server	1
SERVER-OTHER Cesanta Mongoose parse_mqtt Out of Bounds Read	CVE-2019-12951	Other Web Server	2
SERVER-OTHER Cisco ASA VPN aggregateAuthDataHandler double free attempt	CVE-2018-0101	Other Web Server	1
SERVER-OTHER Cisco ASA VPN aggregateAuthDataHandler double free attempt	CVE-2018-0101	Other Web Server	1

SERVER-OTHER Cisco Prime Infrastructure and EPNM UploadServlet Tar Directory Traversal	CVE-2019-1821	Other Web Server	2
SERVER-OTHER Cisco Prime Infrastructure and EPNM UploadServlet Tar Directory Traversal (Published Exploit) (Decrypted Traffic)	CVE-2019-1821	Other Web Server	2
SERVER-OTHER Cisco Prime Infrastructure swimtemp CVE-2018-15379 TFTP Arbitrary File Upload		Other Web Server	2
SERVER-OTHER Cisco Prime Infrastructure swimtemp CVE-2018-15379 TFTP Arbitrary File Upload	CVE-2018-15379	Other Web Server	2
SERVER-OTHER Cisco Smart Install init discovery message stack buffer overflow attempt CVE-2018-0171	CVE-2018-0171	Other Web Server	1
SERVER-OTHER CloudMe Sync Client stack buffer overflow attempt	CVE-2018-6892	Other Web Server	1
SERVER-OTHER Disk Savvy Enterprise buffer overflow attempt		Other Web Server	1
SERVER-OTHER Elastic	CVE-2018-	Web Services	3

Kibana server.js Local File Inclusion	17246	and Applications	
SERVER-OTHER Ethereal Distcc SERR buffer overflow attempt		Other Web Server	1
SERVER-OTHER Fatek Automation PLC WinProladder buffer overflow attempt	CVE-2016-8377	Other Web Server	2
SERVER-OTHER Flexera FlexNet License Server buffer overflow attempt		Other Web Server	1
SERVER-OTHER Fortinet FortiOS appliedTags field cross site scripting attempt		Other Web Server	2
SERVER-OTHER GE Proficy CIMPLICITY Marquee Manager stack buffer overflow attempt		Other Web Server	1
SERVER-OTHER Git CVE-2017-1000117 ssh URL Processing Command Execution Vulnerability	CVE-2017-1000117	Other Web Server	2
SERVER-OTHER Git CVE-2017-1000117 ssh URL Processing Command Execution Vulnerability	CVE-2017-1000117	Other Web Server	4
SERVER-OTHER GitLab Wiki API Attachments Command Injection	CVE-2018-18649	Other Web Server	2
SERVER-OTHER HP AIO Archive Query Server	CVE-2013-6189	Other Web Server	1

stack buffer overflow attempt			
SERVER-OTHER HP Archive Query Server stack overflow attempt	CVE-2011-4163	Other Web Server	1
SERVER-OTHER HP Data Protector Backup Client Service code execution attempt	CVE-2011-0922	Other Web Server	1
SERVER-OTHER HP Data Protector CRS Multiple Opcodes Stack Buffer Overflow	CVE-2013-2324	Other Web Server	1
SERVER-OTHER HP Data Protector CRS Multiple Stack Buffer Overflows	CVE-2013-6195	Other Web Server	1
SERVER-OTHER HP Data Protector CRS Opcode 1091 Stack Buffer Overflow	CVE-2013-2334	Other Web Server	1
SERVER-OTHER HP Data Protector CRS Opcode 215 and 263 Stack Buffer Overflow	CVE-2013-2328	Other Web Server	1
SERVER-OTHER HP Data Protector CRS Opcode 234 Stack Buffer Overflow	CVE-2013-2326	Other Web Server	1
SERVER-OTHER HP Data Protector CRS Opcode 305 Stack Buffer Overflow	CVE-2013-2330	Other Web Server	1
SERVER-OTHER HP Data	CVE-2013-	Other Web	1

Protector EXEC_BAR Command Execution	2347	Server	
SERVER-OTHER HP Data Protector Express Multiple Opcode Parsing Stack Buffer Overflow	CVE-2012-0121	Other Web Server	1
SERVER-OTHER HP Data Protector Opcode 28 and 11 Command Execution	CVE-2014-2623	Other Web Server	1
SERVER-OTHER HP Data Protector client EXEC_CMD command execution attempt	CVE-2011-0923	Other Web Server	1
SERVER-OTHER HP Database Archiving Software GIOP Opcode 0x0E Buffer Overflow	CVE-2011-4163	Other Web Server	1
SERVER-OTHER HP Database Archiving Software GIOP parsing buffer overflow attempt	CVE-2011-4164	Other Web Server	1
SERVER-OTHER HP Integrated Lights-Out HTTP headers processing buffer overflow attempt	CVE-2017-12542	Other Web Server	1
SERVER-OTHER HP Intelligent Management Center dbman BackupDBase opcode command injection attempt	CVE-2017-8954	Other Web Server	1

SERVER-OTHER HP Intelligent Management Center dbman BackupZipFile opcode command injection attempt	CVE-2017-5820	Other Web Server	1
SERVER-OTHER HP Intelligent Management Center dbman CVE-2017-5820 BackupZipFile opcode command injection Vulnerability	CVE-2017-5820	Other Web Server	1
SERVER-OTHER HP Intelligent Management Center dbman RestartDB Opcode Command Injection Attempt	CVE-2017-5816	Other Web Server	1
SERVER-OTHER HP Intelligent Management Center dbman RestoreDBase MSSQL Command Injection	CVE-2017-5817	Other Web Server	2
SERVER-OTHER HP Intelligent Management Center dbman RestoreDBase opcode command injection attempt	CVE-2017-5817	Other Web Server	1
SERVER-OTHER HP Intelligent Management Center dbman buffer overflow attempt	CVE-2011-1850	Other Web Server	1
SERVER-OTHER HP Intelligent Management Center uam.exe stack	CVE-2012-3274	Other Web Server	1

buffer overflow attempt			
SERVER-OTHER HP LeftHand Virtual SAN Appliance hydra Diag Processing Buffer Overflow	CVE-2012-3283	Other Web Server	1
SERVER-OTHER HP LeftHand Virtual SAN Hydra Login Request Buffer Overflow Attempt	CVE-2013-2343	Other Web Server	1
SERVER-OTHER HP LeftHand Virtual SAN hydra diag request buffer overflow attempt	CVE-2012-3283	Other Web Server	1
SERVER-OTHER HP LeftHand Virtual SAN hydra ping request buffer overflow attempt	CVE-2012-3285	Other Web Server	1
SERVER-OTHER HP LoadRunner CVE-2013-4800 Magentproc Stack Buffer Overflow I	CVE-2013-4800	Other Web Server	2
SERVER-OTHER HP LoadRunner CVE-2013-4800 Magentproc Stack Buffer Overflow II	CVE-2013-4800	Other Web Server	2
SERVER-OTHER HP LoadRunner CVE-2013-4800 Magentproc Stack Buffer Overflow III	CVE-2013-4800	Other Web Server	2
SERVER-OTHER HP LoadRunner launcher.dll stack buffer overflow	CVE-2015-2110	Other Web Server	1

attempt			
SERVER-OTHER HP LoadRunner remote command execution attempt	CVE-2010-1549	Other Web Server	1
SERVER-OTHER HP Network Node Manager I ovopi.dll -D Buffer Overflow	CVE-2014-2624	Other Web Server	2
SERVER-OTHER HP Network Node Manager ovopi.dll buffer overflow attempt	CVE-2014-2624	Other Web Server	1
SERVER-OTHER HP OpenView CGI parameter buffer overflow attempt	CVE-2007-6204	Other Web Server	1
SERVER-OTHER HP OpenView NNM nnmRptconfig.exe schdParams and nameParams Buffer Overflow	CVE-2011-0267	Other Web Server	1
SERVER-OTHER HP OpenView Network Node Manager OpenView5 CGI Buffer Overflow	CVE-2008-0067	Other Web Server	1
SERVER-OTHER HP OpenView Network Node Manager netmon.exe Stack Buffer Overflow	CVE-2010-1551	Other Web Server	1
SERVER-OTHER HP OpenView Network	CVE-2011-	Other Web	1

Node Manager nnmRptConfig.exe Template Format String Code Execution	0270	Server	
SERVER-OTHER HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution	CVE-2011-0269	Other Web Server	1
SERVER-OTHER HP OpenView Network Node Manager ovalarm.exe Accept-Language Buffer Overflow	CVE-2009-4179	Other Web Server	1
SERVER-OTHER HP OpenView Network Node Manager ovalarmsrv Integer Overflow	CVE-2008-2438	Other Web Server	1
SERVER-OTHER HP OpenView Network Node Manager ovutil.dll stringToSeconds Buffer Overflow	CVE-2011-0262	Other Web Server	1
SERVER-OTHER HP OpenView Network Node Manager ovwebsnmpsrv.exe OVwSelection Buffer Overflow	CVE-2009-4181	Other Web Server	1
SERVER-OTHER HP OpenView Storage Data Protector CRS opcode 1091 buffer overflow attempt	CVE-2013-2334	Other Web Server	1

SERVER-OTHER HP OpenView Storage Data Protector CRS opcode 1092 buffer overflow attempt	CVE-2013-2331	Other Web Server	1
SERVER-OTHER HP OpenView Storage Data Protector CRS opcode 259 buffer overflow attempt	CVE-2013-2329	Other Web Server	1
SERVER-OTHER HP OpenView Storage Data Protector CRS opcode 264 buffer overflow attempt	CVE-2013-2327	Other Web Server	1
SERVER-OTHER HP OpenView Storage Data Protector exec_cmd buffer overflow attempt	CVE-2011-1866	Other Web Server	1
SERVER-OTHER HP Operations Agent Performance Component Last Chunk Buffer Overflow	CVE-2012-2019	Other Web Server	1
SERVER-OTHER HP Operations Agent Performance Component Last Chunk Buffer Overflow	CVE-2012-2019	Other Web Server	4
SERVER-OTHER HP Operations Orchestration unauthorized serialized object attempt	CVE-2016-8519	Other Web Server	1
SERVER-OTHER HP	CVE-2009-	Other Web	1

Power Manager Remote Code Execution	2685	Server	
SERVER-OTHER HP ProCurve Manager SNAC UpdateCertificatesServlet Code Execution CVE-2013-4812	CVE-2013-4812	Other Web Server	1
SERVER-OTHER HP ProCurve Manager SNAC UpdateCertificatesServlet Code Execution	CVE-2013-4812	Other Web Server	1
SERVER-OTHER HP ProCurve Manager SNAC UpdateCertificatesServlet Code Execution	CVE-2013-4812	Other Web Server	4
SERVER-OTHER HP ProCurve Manager SNAC UpdateDomainControllerServlet Code Execution	CVE-2013-4811	Other Web Server	4
SERVER-OTHER HP SiteScope SOAP Call runOMAgentCommand Command Injection	CVE-2013-2367	Other Web Server	1
SERVER-OTHER HPE Data Protector EXEC_BAR domain Buffer Overflow	CVE-2016-2006	Other Web Server	1
SERVER-OTHER HPE Data Protector EXEC_BAR username Buffer Overflow	CVE-2016-2005	Other Web Server	1

SERVER-OTHER HPE Intelligent Management Center CVE-2017-8961 PLAT flexFileUpload Arbitrary File Upload	CVE-2017-8961	Other Web Server	3
SERVER-OTHER HPE Intelligent Management Center PLAT RedirectServlet parafile Directory Traversal	CVE-2016-8530	Other Web Server	2
SERVER-OTHER HPE Intelligent Management Center RMI Registry Insecure Deserialization	CVE-2017-5792	Other Web Server	1
SERVER-OTHER HPE Intelligent Management Center TopoDebugServlet Insecure Deserialization		Other Web Server	2
SERVER-OTHER HPE Intelligent Management Center dbman Stack Buffer Overflow	CVE-2018-7115	Other Web Server	2
SERVER-OTHER HPE Intelligent Management Center dbman decryptMsgAes Stack Buffer Overflow CVE-2018-7114	CVE-2018-7114	Other Web Server	2
SERVER-OTHER HPE Intelligent Management Center wmiConfigContent Expression Language Injection CVE-2017-12526	CVE-2017-12526	Other Web Server	2

SERVER-OTHER HPE LoadRunner and Performance Center libxdrutil.dll mxdr_string Heap Buffer Overflow	CVE-2017-5789	Other Web Server	1
SERVER-OTHER HPE Moonshot CVE-2017-8976 Provisioning Manager Appliance khuploadfile.cgi Directory Traversal	CVE-2017-8976	Other Web Server	2
SERVER-OTHER HPE Network 2017-5811 Automation FileServlet Firstpass	CVE-2017-5811	Other Web Server	4
SERVER-OTHER HPE Operations Orchestration backwards-compatibility beanutils Insecure Deserialization	CVE-2017-8994	Other Web Server	1
SERVER-OTHER Heimdal KDC CVE-2017-17439 ASN1 DER Length Denial of Service I	CVE-2017-17439	Other Web Server	2
SERVER-OTHER Heimdal KDC CVE-2017-17439 ASN1 DER Length Denial of Service II	CVE-2017-17439	Other Web Server	2
SERVER-OTHER Heimdal KDC CVE-2017-17439 ASN1 DER Length Denial of Service III	CVE-2017-17439	Other Web Server	2
SERVER-OTHER Heimdal KDC CVE-2017-17439	CVE-2017-17439	Other Web Server	2

ASN1 DER Length Denial of Service IV			
SERVER-OTHER IBM Cognos TM1 Server tm1admsd.exe buffer overflow attempt	CVE-2012-0202	Other Web Server	3
SERVER-OTHER IBM Informix Dynamic Server bts_tracefile Directory Traversal		Other Web Server	1
SERVER-OTHER IBM Informix Dynamic Server index.php testconn Heap Buffer Overflow	CVE-2017-1092	Other Web Server	1
SERVER-OTHER IBM Informix Dynamic Server index.php testconn Heap Buffer Overflow	CVE-2017-1092	Other Web Server	3
SERVER-OTHER IBM Informix Dynamic Server set environment buffer overflow attempt	CVE-2011-1033	Other Web Server	1
SERVER-OTHER IBM Lotus Domino LDAP Heap Buffer Overflow	CVE-2010-0358	Other Web Server	1
SERVER-OTHER IBM Lotus Domino LDAP Integer Overflow I	CVE-2011-0917	Other Web Server	1
SERVER-OTHER IBM Lotus Expeditor cai URI Handler Command Execution	CVE-2008-1965	Other Web Server	1

SERVER-OTHER IBM Lotus Notes URL Handler Command Execution	CVE-2012-2174	Other Web Server	1
SERVER-OTHER IBM QRadar SIEM Authentication Bypass (Decrypted Traffic)	CVE-2018-1418	Other Web Server	2
SERVER-OTHER IBM QRadar SIEM Authentication Bypass-I	CVE-2018-1418	Other Web Server	2
SERVER-OTHER IBM QRadar SIEM Authentication Bypass-II	CVE-2018-1418	Other Web Server	1
SERVER-OTHER IBM Tivoli Directory Server ibmslapd.exe Stack Buffer Overflow Attempt	CVE-2011-1206	Other Web Server	1
SERVER-OTHER IBM Tivoli Endpoint Manager CVE-2014-6140 Mobile Device Management Remote Code Execution Attempt	CVE-2014-6140	Other Web Server	2
SERVER-OTHER IBM Tivoli Storage Manager Client dsmagent.exe NodeName Buffer Overflow	CVE-2008-4828	Other Web Server	1
SERVER-OTHER IBM Tivoli Storage Manager FastBack Mount vault Stack Buffer Overflow	CVE-2015-1896	Other Web Server	1

SERVER-OTHER IBM Tivoli Storage Manager FastBack Mount vault Stack Buffer Overflow	CVE-2015-1896	Other Web Server	4
SERVER-OTHER IBM Tivoli Storage Manager FastBack Server Opcode 1331 lza32 Command Injection	CVE-2015-1938	Other Web Server	1
SERVER-OTHER IBM Tivoli Storage Manager FastBack Server Opcode 4115 Buffer Overflow	CVE-2015-4931	Other Web Server	1
SERVER-OTHER IBM Tivoli Storage Manager FastBack buffer overflow attempt	CVE-2015-1896	Other Web Server	1
SERVER-OTHER IBM Tivoli Storage Manager FastBack command injection attempt	CVE-2015-1949	Other Web Server	1
SERVER-OTHER IBM Tivoli Storage Manager FastBack server denial of service attempt	CVE-2015-8523	Other Web Server	3
SERVER-OTHER IBM Tivoli Storage Manager Fastback buffer overflow attempt	CVE-2015-8519	Other Web Server	1
SERVER-OTHER IBM Tivoli Storage Manager Fastback buffer overflow attempt	CVE-2015-8520	Other Web Server	1
SERVER-OTHER IBM	CVE-2015-	Other Web	1

Tivoli Storage Manager Fastback buffer overflow attempt	8521	Server	
SERVER-OTHER IBM Tivoli Storage Manager Fastback buffer overflow attempt	CVE-2015-8522	Other Web Server	1
SERVER-OTHER IBM Tivoli name overflow attempt	CVE-2009-3853	Other Web Server	1
SERVER-OTHER IBM WebSphere Application Server Commons-Collections Library Remote Code Execution I	CVE-2016-0150	Other Web Server	2
SERVER-OTHER IRC w3wt0rk pitbull perl bot remote command execution attempt		Other Web Server	1
SERVER-OTHER Intel AMT HTTP invalid chunk size attempt	CVE-2020-8758	Other Web Server	2
SERVER-OTHER Intel AMT HTTP negative content-length attempt	CVE-2020-8758	Other Web Server	2
SERVER-OTHER Jackson databind deserialization remote code execution attempt	CVE-2017-17485	Other Web Server	1
SERVER-OTHER Java Library CVE-2016-3642 CommonsCollection Unauthorized Serialized	CVE-2015-3253	Other Web Server	2

Object Attempt			
SERVER-OTHER Jenkins CI Server getOrCreate Policy Bypass	CVE-2018-1999001	Other Web Server	2
SERVER-OTHER Joomla! CMS Policy Bypass and Privilege Escalation Vulnerabilities	CVE-2016-8869	Other Web Server	2
SERVER-OTHER Kubernetes API Proxy Request Handling Privilege Escalation (Decrypted Traffic)	CVE-2018-1002105	Other Web Server	2
SERVER-OTHER Kubernetes API Proxy Request Handling Privilege Escalation (Decrypted Traffic)	CVE-2018-1002105	Other Web Server	4
SERVER-OTHER Kubernetes API Proxy Request Handling Privilege Escalation	CVE-2018-1002105	Other Web Server	2
SERVER-OTHER Kubernetes API Server bypass attempt	CVE-2018-1002105	Other Web Server	2
SERVER-OTHER Lighttpd url-path-2f-decode Denial-Of-Service	CVE-2019-11072	Other Web Server	4
SERVER-OTHER Lotus Domino LDAP Heap Buffer Overflow Attempt	CVE-2010-0358	Other Web Server	1
SERVER-OTHER MIT	CVE-2016-	Other Web	1

Kerberos CVE-2016-3119 kadmind Null Pointer Dereference Vulnerability	3119	Server	
SERVER-OTHER Micro Focus Operations Orchestration information disclosure attempt	CVE-2018-6490	Other Web Server	2
SERVER-OTHER Microsoft Frontpage writeto.cnf access	CVE-2002-1717	Other Web Server	3
SERVER-OTHER Microsoft JET Database Engine CVE-2018-8423 Remote Code Execution Vulnerability	CVE-2018-8423	Other Web Server	2
SERVER-OTHER Microsoft Windows DHCP Server Failover Remote Code Execution	CVE-2019-0785	Other Web Server	1
SERVER-OTHER Microsoft Windows DHCP Server Failover Remote Code Execution	CVE-2019-0785	Other Web Server	4
SERVER-OTHER Microsoft Windows DHCP Server Remote Code Execution	CVE-2019-0725	Other Web Server	2
SERVER-OTHER Microsoft Windows DHCP Server Remote Code Execution	CVE-2019-0725	Other Web Server	4
SERVER-OTHER MiniUPnPd SSDP	CVE-2013-	Other Web	2

request buffer overflow attempt	0229	Server	
SERVER-OTHER Multi-Router Looking Glass remote command injection attempt	CVE-2014-3927	Other Web Server	2
SERVER-OTHER NTP Config Unpeer denial of service attempt	CVE-2017-6463	Other Web Server	3
SERVER-OTHER NTP crypto-NAK denial of service attempt	CVE-2016-4957	Other Web Server	2
SERVER-OTHER NTP decodenetnum assertion failure denial of service attempt	CVE-2015-7855	Other Web Server	1
SERVER-OTHER NTP malformed config request denial of service attempt	CVE-2017-6464	Other Web Server	3
SERVER-OTHER NTP origin timestamp denial of service attempt	CVE-2015-7704	Other Web Server	1
SERVER-OTHER NTPsec ntpd CVE-2019-6443 ctl_getitem Out of Bounds Read	CVE-2019-6443	Other Web Server	2
SERVER-OTHER NTPsec ntpd CVE-2019-6443 ctl_getitem Out of Bounds Read	CVE-2019-6443	Other Web Server	3
SERVER-OTHER NTPsec ntpd process_control	CVE-2019-6444	Other Web Server	1

Out of Bounds Read			
SERVER-OTHER NUUO NVRMini2 stack based buffer overflow attempt	CVE-2018-1149	Other Web Server	2
SERVER-OTHER Netatalk dsi_opensession Attention Quantum Out-of-bounds Write (Published Exploit)	CVE-2018-1160	Other Web Server	1
SERVER-OTHER Netatalk dsi_opensession Attention Quantum Out-of-bounds Write	CVE-2018-1160	Other Web Server	1
SERVER-OTHER Nginx Unit Router Process Heap-based Buffer Overflow	CVE-2019-7401	Other Web Server	2
SERVER-OTHER Novell File Reporter CVE-2012-4956 VOL Tag Heap Buffer Overflow I	CVE-2012-4956	Other Web Server	1
SERVER-OTHER Novell File Reporter CVE-2012-4956 VOL Tag Heap Buffer Overflow II	CVE-2012-4956	Other Web Server	1
SERVER-OTHER Novell Groupwise HTTP response message parsing overflow	CVE-2008-2703	Other Web Server	1
SERVER-OTHER Novell Groupwise internet agent http uri buffer overflow attempt	CVE-2011-0334	Other Web Server	1

SERVER-OTHER Novell ZENWorks configuration management preboot opcode 6C request buffer overflow attempt	CVE-2011-3176	Other Web Server	1
SERVER-OTHER Novell ZENworks Configuration Management PreBoot Service Opcode 4c Request Buffer Overflow	CVE-2011-3176	Other Web Server	1
SERVER-OTHER Novell ZENworks Configuration Management PreBoot Service Opcode 6c Request Buffer Overflow	CVE-2011-3176	Other Web Server	1
SERVER-OTHER Novell ZENworks Configuration Management Preboot service code overflow attempt		Other Web Server	1
SERVER-OTHER Novell eDirectory LDAP NULL Search Parameter Buffer Overflow	CVE-2008-1809	Other Web Server	1
SERVER-OTHER Novell eDirectory NCP stack buffer overflow attempt	CVE-2012-0432	Other Web Server	1
SERVER-OTHER OpenLDAP ldapsearch pagesize Double Free Denial of Service	CVE-2017-9287	Other Web Server	3
SERVER-OTHER OpenLDAP zero size	CVE-2017-9287	Other Web Server	3

PagedResultsControl denial of service attempt			
SERVER-OTHER OpenMRS webservices.rest Insecure Object Deserialization	CVE-2018-19276	Other Web Server	2
SERVER-OTHER OpenSSH CVE-2016-6515 sshd auth_passwd Denial of Service Vulnerability	CVE-2016-6515	Other Web Server	1
SERVER-OTHER Oracle Java JMX server insecure configuration remote code execution attempt	CVE-2015-2342	Other Web Server	1
SERVER-OTHER Oracle Tuxedo Jolt Protocol CVE-2017-10272 Information Disclosure	CVE-2017-10272	Other Web Server	3
SERVER-OTHER Pharos PopUp Printer Client DecodeBinary heap buffer overflow attempt	CVE-2017-2788	Other Web Server	1
SERVER-OTHER Pharos PopUp Printer Client DecodeString denial of service attempt	CVE-2017-2786	Other Web Server	2
SERVER-OTHER Pidgin MXIT protocol handling splash_remove directory traversal attempt	CVE-2016-4323	Other Web Server	2

SERVER-OTHER PostgreSQL Database Password Change Stack Buffer Overflow	CVE-2019-10164	Other Web Server	2
SERVER-OTHER Proface GP-Pro EX EX-ED BeginPreRead stack buffer overflow attempt	CVE-2016-2292	Other Web Server	3
SERVER-OTHER Quest Privilege Manager pmmasterd buffer overflow attempt	CVE-2017-6553	Other Web Server	1
SERVER-OTHER RaySharp CCTV derivative command injection attempt		Other Web Server	1
SERVER-OTHER Red Hat librelp Stack Buffer Overflow	CVE-2018-1000140	Other Web Server	2
SERVER-OTHER Redis lua script integer overflow attempt	CVE-2015-8080	Other Web Server	3
SERVER-OTHER Rockwell Automation RSLinx Classic Forward Open Electronic Key Stack Buffer Overflow	CVE-2019-6553	Other Web Server	2
SERVER-OTHER Rsync CVE-2017-16548 eceive_xattr Heap-based Buffer Overread	CVE-2017-16548	Other Web Server	2
SERVER-OTHER Rsync CVE-2017-16548 receive_xattr Heap-	CVE-2017-16548	Other Web Server	4

based Buffer Overread			
SERVER-OTHER Samba CVE-2018-1057 LDAP AD DC Privilege Escalation	CVE-2018-1057	Other Web Server	2
SERVER-OTHER Squid HTTP Accept Encoding response header denial of service attempt	CVE-2016-3948	Other Web Server	2
SERVER-OTHER Tipping Point IPS reverse DNS lookup format string exploit attempt		Other Web Server	1
SERVER-OTHER Trend Micro Control Manager XML External Entity Processing (Decrypted Traffic)		Other Web Server	1
SERVER-OTHER Trend Micro Mobile Security Enterprise get_dep_profile id SQL Injection I	CVE-2017-14078	Other Web Server	2
SERVER-OTHER Trend Micro Mobile Security Enterprise get_dep_profile id SQL Injection II	CVE-2017-14078	Other Web Server	2
SERVER-OTHER UltraVNC VNC Server CVE-2019-8274 File Transfer Offer Handler Heap-based Buffer Overflow	CVE-2019-8274	Other Web Server	2

SERVER-OTHER UltraVNC VNC Server CVE-2019-8274 File Transfer Offer Handler Heap-based Buffer Overflow	CVE-2019-8274	Other Web Server	4
SERVER-OTHER Verso NetPerformer frame relay access device telnet buffer overflow attempt		Other Web Server	1
SERVER-OTHER Western Digital My Cloud authentication bypass attempt	CVE-2018-17153	Other Web Server	2
SERVER-OTHER Wordpress CMS platform denial of service attempt	CVE-2018-6389	Other Web Server	1
SERVER-OTHER Xi Software Net Transport eDonkey Protocol Buffer Overflow attempt		Other Web Server	1
SERVER-OTHER Zoho ManageEngine OpManager APIDBUtil getDevicesForSearchString SQL Injection	CVE-2018-17243	Other Web Server	2
SERVER-OTHER Zoho ManageEngine OpManager Business View Background Image Arbitrary File Upload	CVE-2018-18475	Other Web Server	2
SERVER-OTHER dhcpcd DHCPv6 CVE-2019-	CVE-2019-11577	Other Web Server	2

11577 dhcp6_findna Buffer Overflow			
SERVER-OTHER libVNC LibVNCClient CoRRE Heap-based Buffer Overflow CVE-2018-20020	CVE-2018-20020	Other Web Server	2
SERVER-OTHER libVNC LibVNCClient CoRRE Heap-based Buffer Overflow CVE-2018-20020	CVE-2018-20020	Other Web Server	4
SERVER-OTHER libVNC LibVNCServer File Transfer Extension Heap-based Buffer Overflow	CVE-2018-15127	Other Web Server	2
SERVER-OTHER libVNC LibVNCServer File Transfer Extension Heap-based Buffer Overflow	CVE-2018-15127	Other Web Server	4
SERVER-OTHER limited RSA ciphersuite list - possible Bleichenbacher SSL attack attempt	CVE-2012-5081	Other Web Server	3
SERVER-OTHER ntpd mrulist control message command null pointer dereference attempt	CVE-2016-7434	Other Web Server	3
SERVER-OTHER ntpd saveconfig directory traversal attempt	CVE-2015-7851	Other Web Server	2
SERVER-OTHER tcpdump ISAKMP parser	CVE-2017-	Other Web	1

buffer overflow attempt	5205	Server	
SERVER-SAMBA Samba LDAP AD DC Nested Filter CVE-2020-10704 Denial of Service	CVE-2020-10704	Web Services and Applications	2
SERVER-SAMBA Samba LDAP AD DC Privilege Escalation (Decrypted Traffic)	CVE-2018-1057	Operating System and Services	1
SERVER-SAMBA Samba LDAP AD DC Privilege Escalation (Decrypted Traffic)	CVE-2018-1057	Operating System and Services	2
SERVER-SAMBA Samba NDR Parsing ndr_pull_dnsp_name Integer Overflow	CVE-2016-2123	Operating System and Services	2
SERVER-SAMBA Samba SMB1 smb_request_done Use After Free	CVE-2017-14746	Operating System and Services	3
SERVER-WEBAPP Adobe ColdFusion CVE-2018-15959 DataServicesCFProxy Commons BeanUtils Insecure Deserialization	CVE-2018-15959	Web Services and Applications	2
SERVER-WEBAPP Adobe ColdFusion CVE-2018-15959 DataServicesCFProxy Commons BeanUtils Insecure Deserialization	CVE-2018-15959	Web Services and Applications	3
SERVER-WEBAPP Adobe ColdFusion CVE-2019-	CVE-2019-	Web Services and	2

7091 JavaAdapter JavaBeanAdapter Insecure Deserialization	7091	Applications	
SERVER-WEBAPP AlienVault OSSIM API get_host_fqdn host_ip command injection attempt		Web Services and Applications	1
SERVER-WEBAPP AlienVault USM and OSSIM fqdn get_fqdn Command Injection (Decrypted Traffic)		Web Services and Applications	1
SERVER-WEBAPP AlienVault USM and OSSIM fqdn get_fqdn Command Injection I		Web Services and Applications	2
SERVER-WEBAPP AlienVault USM and OSSIM fqdn get_fqdn Command Injection II		Web Services and Applications	2
SERVER-WEBAPP AlienVault USM and OSSIM fqdn get_fqdn Command Injection III		Web Services and Applications	2
SERVER-WEBAPP Alienvault CVE-2016-8582 Unified Security Management and OSSIM gauge.php SQL Injection	CVE-2016-8582	Web Services and Applications	2
SERVER-WEBAPP Alienvault OSSIM gauge.php value SQL injection attempt	CVE-2016-8582	Web Services and Applications	2

SERVER-WEBAPP Apache CVE-2016-1000031 Commons Library FileUpload unauthorized Java object upload attempt	CVE-2016-1000031	Web Services and Applications	2
SERVER-WEBAPP Apache OFBiz stream contentId (CVE-2020-1943)Cross-Site Scripting (Decrypted Traffic)	CVE-2020-1943	Web Services and Applications	1
SERVER-WEBAPP Apache OFBiz stream contentId (CVE-2020-1943)Cross-Site Scripting (Encrypted Traffic)	CVE-2020-1943	Web Services and Applications	1
SERVER-WEBAPP Apache Struts XSLTResult File Inclusion	CVE-2016-3082	Web Services and Applications	1
SERVER-WEBAPP Apache Subversion mod_authz_svn COPY MOVE Denial of Service	CVE-2016-2168	Web Services and Applications	3
SERVER-WEBAPP Apache Superset python pickle library remote code execution attempt	CVE-2018-8021	Apache HTTP Server	1
SERVER-WEBAPP Apache Superset python pickle library remote code execution attempt	CVE-2018-8021	Web Services and Applications	1

SERVER-WEBAPP Apache Superset python pickle library remote code execution attempt	CVE-2018-8021	Web Services and Applications	2
SERVER-WEBAPP Apache TomEE java deserialization attempt	CVE-2016-0779	Web Services and Applications	1
SERVER-WEBAPP Apache Tomcat FileStore directory traversal attempt	CVE-2020-9484	Web Services and Applications	1
SERVER-WEBAPP Belkin F9K1122 webpage buffer overflow attempt		Web Services and Applications	1
SERVER-WEBAPP Belkin Wemo UPnP command injection attempt	CVE-2019-12780	Web Services and Applications	2
SERVER-WEBAPP Borland AccuRev Reprise License Server directory traversal attempt		Web Services and Applications	2
SERVER-WEBAPP Borland AccuRev SaveContentServiceImpl servlet directory traversal attempt		Web Services and Applications	2
SERVER-WEBAPP CA Total Defense Suite UNCWS Multiple Report Stored Procedure SQL Injections	CVE-2011-1653	Web Services and Applications	1
SERVER-WEBAPP CA	CVE-2011-	Web Services	2

Total Defense Suite UNCWS UnassignFunctionalRoles Stored Procedure POST SQL Injection Attempt	1653	and Applications	
SERVER-WEBAPP CA Total Defense Suite UNCWS UnassignFunctionalRoles Stored Procedure SQL Injection Attempt	CVE-2011-1653	Web Services and Applications	2
SERVER-WEBAPP CA Total Defense Suite UNCWS UnassignFunctionalRoles Stored Procedure SQL Injection	CVE-2011-1653	Web Services and Applications	1
SERVER-WEBAPP CA Total Defense management.asmx sql injection attempt	CVE-2011-1653	Web Services and Applications	1
SERVER-WEBAPP CA Unified Infrastructure Management download_lar.jsp Directory Traversal	CVE-2016-5803	Web Services and Applications	2
SERVER-WEBAPP CA eHealth command injection attempt	CVE-2016-6152	Web Services and Applications	2
SERVER-WEBAPP CA eHealth command injection command injection attempt	CVE-2016-6152	Web Services and Applications	2
SERVER-WEBAPP CGit CVE-2018-14912	CVE-2018-	Web Services and	3

cgit_clone_objects function directory traversal attempt	14912	Applications	
SERVER-WEBAPP Cisco 220 Series Smart Switches command injection attempt	CVE-2019-1914	Web Services and Applications	1
SERVER-WEBAPP Cisco 220 Series Smart Switches stack buffer overflow attempt	CVE-2019-1913	Web Services and Applications	1
SERVER-WEBAPP Cisco 220 Series Smart Switches stack buffer overflow attempt	CVE-2019-1913	Web Services and Applications	2
SERVER-WEBAPP Cisco ASA WebVPN expired session page direct access denial of service attempt	CVE-2019-1693	Web Services and Applications	1
SERVER-WEBAPP Cisco ASA and FTD denial of service attempt	CVE-2020-3572	Web Services and Applications	2
SERVER-WEBAPP Cisco ASA and FTD directory traversal attempt	CVE-2020-3187	Web Services and Applications	1
SERVER-WEBAPP Cisco ASA and FTD web services large file upload denial of service attempt	CVE-2020-3436	Web Services and Applications	2
SERVER-WEBAPP Cisco ASA secure desktop login denial of service	CVE-2018-15388	Web Services and Applications	1

attempt			
SERVER-WEBAPP Cisco Adaptive Security Appliance Webvpn XML Parser Double Free (Decrypted Traffic) CVE-2018-0101	CVE-2018-0101	Web Services and Applications	2
SERVER-WEBAPP Cisco Adaptive Security Appliance Webvpn XML Parser Double Free CVE-2018-0101	CVE-2018-3609	Web Services and Applications	2
SERVER-WEBAPP Cisco Adaptive Security Appliance admin command interface access attempt	CVE-2019-1713	Web Services and Applications	2
SERVER-WEBAPP Cisco Cloud Services Platform dnslookup command injection attempt	CVE-2016-6374	Web Services and Applications	2
SERVER-WEBAPP Cisco DDR2200 ADSL gateway command injection attempt	CVE-2017-11588	Web Services and Applications	1
SERVER-WEBAPP Cisco Data Center Network Manager LanFabricImpl createLanFabric command injection attempt	CVE-2019-15978	Web Services and Applications	1
SERVER-WEBAPP Cisco Data Center Network Manager SQL injection attempt	CVE-2019-15984	Web Services and Applications	1

SERVER-WEBAPP Cisco Data Center Network Manager SQL injection attempt	CVE-2019-15984	Web Services and Applications	2
SERVER-WEBAPP Cisco Data Center Network Manager SecurityManager Authentication Bypass (Decrypted Traffic)	CVE-2019-15976	Web Services and Applications	1
SERVER-WEBAPP Cisco Data Center Network Manager SecurityManager Authentication Bypass	CVE-2019-15976	Web Services and Applications	1
SERVER-WEBAPP Cisco Data Center Network Manager TrustedClientTokenValidator Authentication Bypass (Decrypted Traffic)	CVE-2019-15975	Web Services and Applications	1
SERVER-WEBAPP Cisco Data Center Network Manager TrustedClientTokenValidator Authentication Bypass (encrypted Traffic)	CVE-2019-15975	Web Services and Applications	1
SERVER-WEBAPP Cisco Data Center Network Manager arbitrary WAR file upload attempt	CVE-2019-1620	Web Services and Applications	1
SERVER-WEBAPP Cisco Data Center Network Manager authentication	CVE-2019-1619	Web Services and Applications	1

bypass attempt			
SERVER-WEBAPP Cisco Data Center Network Manager command injection attempt	CVE-2020-3384	Web Services and Applications	1
SERVER-WEBAPP Cisco Data Center Network Manager createLanFabric CVE-2019-15978 Command Injection	CVE-2019-15978	Web Services and Applications	1
SERVER-WEBAPP Cisco Data Center Network Manager directory traversal attempt	CVE-2020-3383	Web Services and Applications	2
SERVER-WEBAPP Cisco Data Center Network Manager getConfigTemplateFileName CVE-2019-15984 SQL Injection (Decrypted Traffic)	CVE-2019,15984	Web Services and Applications	3
SERVER-WEBAPP Cisco Data Center Network Manager getConfigTemplateFileName CVE-2019-15984 SQL Injection		Web Services and Applications	3
SERVER-WEBAPP Cisco Data Center Network Manager getConfigTemplateFileName CVE-2019-15984 SQL Injection	CVE-2019-15984	Web Services and Applications	3
SERVER-WEBAPP Cisco Data Center Network	CVE-2019-	Web Services and	1

Manager getLicenses SQL Injection (Decrypted Traffic)	15984	Applications	
SERVER-WEBAPP Cisco Data Center Network Manager getLicenses SQL Injection	CVE-2019-15984	Web Services and Applications	1
SERVER-WEBAPP Cisco Data Center Network Manager getSwitchsDataLength (CVE-2019-15984) SQL Injection (Decrypted Traffic)	CVE-2019-15984	Web Services and Applications	1
SERVER-WEBAPP Cisco Data Center Network Manager getSwitchsDataLength (CVE-2019-15984) SQL Injection (Encrypted Traffic)		Web Services and Applications	1
SERVER-WEBAPP Cisco Data Center Network Manager getTokenInfo CVE-2019-15984 SQL Injection (Decrypted Traffic)	CVE-2019-15984	Web Services and Applications	1
SERVER-WEBAPP Cisco Data Center Network Manager getTokenInfo CVE-2019-15984 SQL Injection	CVE-2019-15984	Web Services and Applications	1
SERVER-WEBAPP Cisco Data Center Network Manager importTS CVE-2019-15979 Command Injection		Web Services and Applications	1

SERVER-WEBAPP Cisco Data Center Network Manager importTS CVE-2019-15979 Command Injection	CVE-2019-15979	Web Services and Applications	1
SERVER-WEBAPP Cisco Data Center Network Manager persistUserInfo CVE-2019-15984 SQL Injection (Decrypted Traffic)	CVE-2019-15984	Web Services and Applications	3
SERVER-WEBAPP Cisco Data Center Network Manager persistUserInfo CVE-2019-15984 SQL Injection	CVE-2019-15984	Web Services and Applications	1
SERVER-WEBAPP Cisco Data Center Network Manager persistUserInfo CVE-2019-15984 SQL Injection	CVE-2019-15984	Web Services and Applications	3
SERVER-WEBAPP Cisco Elastic Services Controller REST API Authentication Bypass	CVE-2019-1867	Web Services and Applications	2
SERVER-WEBAPP Cisco Elastic Services Controller authentication bypass attempt	CVE-2019-1867	Web Services and Applications	2
SERVER-WEBAPP Cisco Enterprise NFV command injection	CVE-2019-1893	Web Services and Applications	1

attempt			
SERVER-WEBAPP Cisco Firepower Management Center LDAP authentication bypass attempt	CVE-2019-16028	Web Services and Applications	1
SERVER-WEBAPP Cisco Firepower Management Center SQL injection attempt	CVE-2019-12679	Web Services and Applications	1
SERVER-WEBAPP Cisco Firepower Management Center SQL injection attempt	CVE-2019-12680	Web Services and Applications	1
SERVER-WEBAPP Cisco Firepower Management Center SQL injection attempt	CVE-2019-12681	Web Services and Applications	1
SERVER-WEBAPP Cisco Firepower Management Center SQL injection attempt	CVE-2019-12682	Web Services and Applications	1
SERVER-WEBAPP Cisco Firepower Management Center SQL injection attempt	CVE-2019-12683	Web Services and Applications	1
SERVER-WEBAPP Cisco Firepower Management Center SQL injection attempt	CVE-2019-12684	Web Services and Applications	1
SERVER-WEBAPP Cisco Firepower Management Center command injection attempt	CVE-2019-12687	Web Services and Applications	1

SERVER-WEBAPP Cisco Firepower Management Center command injection attempt	CVE-2019-12690	Web Services and Applications	1
SERVER-WEBAPP Cisco Firepower Management Center directory traversal attempt	CVE-2019-12689	Web Services and Applications	1
SERVER-WEBAPP Cisco IOS XE REST API information disclosure attempt	CVE-2019-12643	Web Services and Applications	1
SERVER-WEBAPP Cisco IOS XE Software command injection attempt	CVE-2019-12651	Web Services and Applications	1
SERVER-WEBAPP Cisco IOS XE Web UI command injection attempt	CVE-2019-1862	Web Services and Applications	2
SERVER-WEBAPP Cisco IOS XE Web UI command injection attempt	CVE-2020-3211	Web Services and Applications	1
SERVER-WEBAPP Cisco IOS XE Web UI command injection attempt	CVE-2020-3212	Web Services and Applications	1
SERVER-WEBAPP Cisco IOS XE Web UI command injection attempt	CVE-2020-3219	Web Services and Applications	1
SERVER-WEBAPP Cisco IOS XE WebUI	CVE-2019-12651	Web Services and	2

Command Injection Vulnerability		Applications	
SERVER-WEBAPP Cisco IOS XE WebUI Privileged Command Injection Vulnerability	CVE-2019-12650	Web Services and Applications	1
SERVER-WEBAPP Cisco IOS XE denial of service attempt	CVE-2018-0191	Web Services and Applications	3
SERVER-WEBAPP Cisco IOS XE webui cdp resource command injection attempt	CVE-2019-1755	Web Services and Applications	1
SERVER-WEBAPP Cisco IOS XE webui debugBundle command injection attempt	CVE-2019-1753	Apache HTTP Server	2
SERVER-WEBAPP Cisco IOS XE webui debugBundle command injection attempt	CVE-2019-1753	Web Services and Applications	1
SERVER-WEBAPP Cisco IOS XE webui debugBundle command injection attempt	CVE-2019-1753	Web Services and Applications	2
SERVER-WEBAPP Cisco IOS XE webui dhcp resource command injection attempt	CVE-2019-1755	Apache HTTP Server	2
SERVER-WEBAPP Cisco IOS XE webui directory traversal attempt	CVE-2019-1743	Web Services and Applications	1
SERVER-WEBAPP Cisco	CVE-2019-	Apache HTTP	2

IOS XE webui rathrottler command injection attempt	1754	Server	
SERVER-WEBAPP Cisco IOS XE webui rathrottler command injection attempt	CVE-2019-1754	Web Services and Applications	1
SERVER-WEBAPP Cisco IOS XE webui rathrottler command injection attempt	CVE-2019-1754	Web Services and Applications	2
SERVER-WEBAPP Cisco IP Phone CVE-2020-3161 libHTTPService.so Stack Buffer Overflow	CVE-2020-3161	Web Services and Applications	2
SERVER-WEBAPP Cisco IP Phone libHTTPService.so stack buffer overflow attempt	CVE-2020-3161	Web Services and Applications	2
SERVER-WEBAPP Cisco IP Phone web interface stack buffer overflow attempt	CVE-2019-1716	Web Services and Applications	1
SERVER-WEBAPP Cisco Industrial Network Director remote code execution attempt	CVE-2019-1861	Web Services and Applications	2
SERVER-WEBAPP Cisco Integrated Management Controller Redfish API command injection attempt	CVE-2019-1885	Web Services and Applications	1
SERVER-WEBAPP Cisco Integrated Management Controller	CVE-2019-1907	Web Services and	1

authentication bypass attempt		Applications	
SERVER-WEBAPP Cisco Integrated Management Controller buffer overflow attempt	CVE-2019-1871	Web Services and Applications	1
SERVER-WEBAPP Cisco Integrated Management Controller command injection attempt	CVE-2018-0430	Web Services and Applications	1
SERVER-WEBAPP Cisco Integrated Management Controller command injection attempt	CVE-2019-1864	Web Services and Applications	1
SERVER-WEBAPP Cisco Integrated Management Controller command injection attempt	CVE-2019-1896	Web Services and Applications	1
SERVER-WEBAPP Cisco Integrated Management Controller denial of service attempt	CVE-2019-1900	Web Services and Applications	1
SERVER-WEBAPP Cisco NX-OS Software NX-API denial of service attempt	CVE-2019-1968	Web Services and Applications	1
SERVER-WEBAPP Cisco NX-OS System Software NX-API command injection attempt	CVE-2019-1614	Web Services and Applications	2
SERVER-WEBAPP Cisco Prime Collaboration Assurance unauthorized access attempt	CVE-2019-1662	Web Services and Applications	1

SERVER-WEBAPP Cisco Prime Collaboration Provisioning SQL injection attempt	CVE-2018-0320	Web Services and Applications	1
SERVER-WEBAPP Cisco Prime Collaboration Provisioning SQL injection attempt	CVE-2018-0320	Web Services and Applications	2
SERVER-WEBAPP Cisco Prime Data Center Network Manager fileUpload Arbitrary File Upload (Decrypted Traffic)	CVE-2019-1620	Web Services and Applications	1
SERVER-WEBAPP Cisco Prime Data Center Network Manager fileUpload Arbitrary File Upload (encrypted Traffic)	CVE-2019-1620	Web Services and Applications	3
SERVER-WEBAPP Cisco Prime Infrastructure Health Monitor TarArchive CVE-2019-1821 Directory Traversal	CVE-2019-1821	Web Services and Applications	1
SERVER-WEBAPP Cisco Prime Infrastructure SQL injection attempt	CVE-2019-1824	Web Services and Applications	2
SERVER-WEBAPP Cisco Prime Infrastructure directory traversal attempt	CVE-2018-0258	Web Services and Applications	1
SERVER-WEBAPP Cisco Prime Infrastructure directory traversal	CVE-2018-0258	Web Services and Applications	2

attempt			
SERVER-WEBAPP Cisco Prime Infrastructure directory traversal attempt	CVE-2019-15958	Web Services and Applications	1
SERVER-WEBAPP Cisco Prime License Manager SQL injection attempt	CVE-2018-15441	Web Services and Applications	1
SERVER-WEBAPP Cisco Prime License Manager SQL injection attempt	CVE-2018-15441	Web Services and Applications	2
SERVER-WEBAPP Cisco Prime Network Analysis Module command injection attempt	CVE-2016-1388	Web Services and Applications	2
SERVER-WEBAPP Cisco Prime Service Catalog cross site request forgery attempt	CVE-2019-1874	Web Services and Applications	1
SERVER-WEBAPP Cisco Prime Service Catalog cross site scripting attempt	CVE-2019-1874	Web Services and Applications	1
SERVER-WEBAPP Cisco RV Series Routers authentication bypass attempt	CVE-2020-3144	Web Services and Applications	1
SERVER-WEBAPP Cisco RV Series Routers command injection attempt	CVE-2016-1395	Web Services and Applications	1
SERVER-WEBAPP Cisco RV Series Routers	CVE-2019-15271	Web Services and	1

command injection attempt		Applications	
SERVER-WEBAPP Cisco RV Series Routers command injection attempt	CVE-2019-1652	Web Services and Applications	2
SERVER-WEBAPP Cisco RV Series Routers command injection attempt	CVE-2020-3268	Web Services and Applications	1
SERVER-WEBAPP Cisco RV Series Routers command injection attempt	CVE-2020-3274	Web Services and Applications	1
SERVER-WEBAPP Cisco RV Series Routers command injection attempt	CVE-2020-3332	Web Services and Applications	1
SERVER-WEBAPP Cisco RV Series Routers denial of service attempt	CVE-2019-1843	Web Services and Applications	1
SERVER-WEBAPP Cisco RV Series Routers heap buffer overflow attempt	CVE-2020-3357	Web Services and Applications	1
SERVER-WEBAPP Cisco RV Series Routers null pointer dereference attempt	CVE-2020-3358	Web Services and Applications	1
SERVER-WEBAPP Cisco RV Series Routers stack buffer overflow attempt	CVE-2019-1663	Web Services and Applications	1
SERVER-WEBAPP Cisco RV Series Routers stack	CVE-2020-3145	Web Services and	2

buffer overflow attempt		Applications	
SERVER-WEBAPP Cisco RV Series Routers stack buffer overflow attempt	CVE-2020-3269	Web Services and Applications	2
SERVER-WEBAPP Cisco RV Series Routers stack buffer overflow attempt	CVE-2020-3286	Web Services and Applications	1
SERVER-WEBAPP Cisco RV Series Routers stack buffer overflow attempt	CVE-2020-3287	Web Services and Applications	2
SERVER-WEBAPP Cisco RV Series Routers stack buffer overflow attempt	CVE-2020-3288	Web Services and Applications	1
SERVER-WEBAPP Cisco RV Series Routers stack buffer overflow attempt	CVE-2020-3288	Web Services and Applications	2
SERVER-WEBAPP Cisco RV Series Routers stack buffer overflow attempt	CVE-2020-3323	Web Services and Applications	1
SERVER-WEBAPP Cisco RV132W and RV134W routers command injection attempt	CVE-2018-0125	Web Services and Applications	2
SERVER-WEBAPP Cisco SD-WAN Solution command injection attempt	CVE-2019-1624	Web Services and Applications	1
SERVER-WEBAPP Cisco SD-WAN Solution vManage CVE-2019-16012 SQL Injection	CVE-2019-16012	Web Services and Applications	1
SERVER-WEBAPP Cisco	CVE-2019-	Web Services	2

SD-WAN Solution vManage CVE-2019-16012 SQL Injection	16012	and Applications	
SERVER-WEBAPP Cisco SD-WAN vManage SQL injection attempt	CVE-2019-16012	Web Services and Applications	1
SERVER-WEBAPP Cisco SD-WAN vManage cypher query language injection attempt	CVE-2020-3387	Web Services and Applications	1
SERVER-WEBAPP Cisco SD-WAN vManage directory traversal attempt	CVE-2020-26073	Web Services and Applications	1
SERVER-WEBAPP Cisco SPA100 Series analog telephone adapters buffer overflow attempt	CVE-2019-15240	Web Services and Applications	1
SERVER-WEBAPP Cisco Security Manager RMI Insecure Deserialization	CVE-2019-12630	Web Services and Applications	4
SERVER-WEBAPP Cisco Small Business Series Switches denial of service attempt	CVE-2019-1891	Web Services and Applications	1
SERVER-WEBAPP Cisco Small Business Series Switches denial of service attempt	CVE-2020-3147	Web Services and Applications	1
SERVER-WEBAPP Cisco Small Business Switches cross site scripting attempt	CVE-2019-12636	Web Services and Applications	1

SERVER-WEBAPP Cisco Small Business Switches denial of service attempt	CVE-2019-12636	Web Services and Applications	1
SERVER-WEBAPP Cisco Smart Software Manager denial of service attempt	CVE-2019-16029	Web Services and Applications	1
SERVER-WEBAPP Cisco Smart Software Manager unauthorized password change attempt	CVE-2019-16029	Web Services and Applications	1
SERVER-WEBAPP Cisco UCS Director ApplianceStorageUtil unzip(CVE-2020-3239) Directory Traversal	CVE-2020-3239	Web Services and Applications	1
SERVER-WEBAPP Cisco UCS Director ApplianceStorageUtil unzip(CVE-2020-3239) Directory Traversal	CVE-2020-3239	Web Services and Applications	5
SERVER-WEBAPP Cisco UCS Director CopyFileRunnable run Symlink CVE-2020-3247 Remote Code Execution (Decrypted Traffic)	CVE-2020-3247	Web Services and Applications	2
SERVER-WEBAPP Cisco UCS Director CopyFileRunnable run Symlink CVE-2020-3247 Remote Code Execution	CVE-2020-3247	Web Services and Applications	2
SERVER-WEBAPP Cisco	CVE-2020-	Web Services	2

UCS Director LargeFileUploadServlet directory traversal attempt	3239	and Applications	
SERVER-WEBAPP Cisco UCS Director LargeFileUploadServlet directory traversal attempt	CVE-2020-3247	Web Services and Applications	2
SERVER-WEBAPP Cisco UCS Director MyCallable call CVE-2020-3251 Directory Traversal (Decrypted Traffic)	CVE-2020-3251	Web Services and Applications	2
SERVER-WEBAPP Cisco UCS Director MyCallable call CVE-2020-3251 Directory Traversal (Encrypted Traffic)	CVE-2020-3251	Web Services and Applications	2
SERVER-WEBAPP Cisco UCS Director REST API directory traversal attempt	CVE-2020-3250	Web Services and Applications	2
SERVER-WEBAPP Cisco UCS Director arbitrary JSP file upload attempt	CVE-2020-3251	Web Services and Applications	2
SERVER-WEBAPP Cisco UCS Director authentication bypass attempt	CVE-2019-1974	Web Services and Applications	1
SERVER-WEBAPP Cisco UCS Director authentication bypass attempt	CVE-2020-3243	Web Services and Applications	2

SERVER-WEBAPP Cisco UCS Director downloadFile (CVE-2020-3250)Directory Traversal	CVE-2020-3250	Web Services and Applications	1
SERVER-WEBAPP Cisco UCS Director downloadFile (CVE-2020-3250)Directory Traversal(Decrypted Traffic)	CVE-2020-3250	Web Services and Applications	1
SERVER-WEBAPP Cisco UCS Director isEnableRestKeyAccessCheckForUser Authentication Bypass Vulnerability	CVE-2020-3243	Web Services and Applications	2
SERVER-WEBAPP Cisco UCS Director saveStaticConfig CVE-2020-3248 Directory Traversal		Web Services and Applications	3
SERVER-WEBAPP Cisco Ultra Services Framework command injection attempt	CVE-2017-6714	Web Services and Applications	1
SERVER-WEBAPP Cisco Unified Contact Center Express RMI (CVE-2020-3280) Insecure Deserialization	CVE- 2020-3280	Web Services and Applications	5
SERVER-WEBAPP Cisco Unified Contact Center Express RMI (CVE-2020-3280) Insecure Deserialization	CVE-2020-3280	Web Services and Applications	1

SERVER-WEBAPP Cisco Unity Express RMI Insecure Deserialization CVE-2018-15381	CVE-2018-15381	Web Services and Applications	2
SERVER-WEBAPP Cisco Unity Express RMI Insecure Deserialization CVE-2018-15381	CVE-2018-15381	Web Services and Applications	4
SERVER-WEBAPP Cisco Vision Dynamic Signage Director authentication bypass attempt	CVE-2019-1917	Web Services and Applications	1
SERVER-WEBAPP Cisco Web Security Appliance command injection attempt	CVE-2019-1816	Web Services and Applications	1
SERVER-WEBAPP Cisco Web Security Appliance command injection attempt	CVE-2019-1816	Web Services and Applications	2
SERVER-WEBAPP Cisco Web Security Appliance denial of service attempt	CVE-2019-1884	Web Services and Applications	1
SERVER-WEBAPP Cisco Web Security Appliance proxy service buffer overflow attempt	CVE-2019-1817	Web Services and Applications	1
SERVER-WEBAPP Cisco WebVPN denial of service attempt	CVE-2019-12698	Web Services and Applications	1
SERVER-WEBAPP Cisco Webex Video Mesh Node command	CVE-2019-16005	Web Services and Applications	1

injection attempt			
SERVER-WEBAPP Cisco Wireless LAN Controller cross site request forgery attempt	CVE-2019-1797	Web Services and Applications	2
SERVER-WEBAPP Cisco Wireless LAN Controller denial of service attempt	CVE-2018-0248	Web Services and Applications	1
SERVER-WEBAPP Cisco Wireless LAN Controller denial of service attempt	CVE-2018-0248	Web Services and Applications	3
SERVER-WEBAPP Cisco Wireless LAN Controller denial of service attempt	CVE-2019-15276	Web Services and Applications	1
SERVER-WEBAPP Citrix Application Delivery Controller and Gateway Directory Traversal (encrypted Traffic)	CVE-2019-19781	Web Services and Applications	1
SERVER-WEBAPP D-Link Central WiFi Manager CMW 100 cross site scripting attempt	CVE-2019-13374	Web Services and Applications	1
SERVER-WEBAPP D-Link DIR Series Routers HNAP stack buffer overflow attempt	CVE-2016-6563	Web Services and Applications	1
SERVER-WEBAPP D-Link DIR-620 CVE-2018-6211 index.cgi command injection attempt	CVE-2018-6211	Web Services and Applications	3

SERVER-WEBAPP D-Link DIR-620 index.cgi command injection attempt	CVE-2018-6211	Web Services and Applications	2
SERVER-WEBAPP D-Link DIR-816 diagnosis command injection attempt	CVE-2018-17068	Web Services and Applications	2
SERVER-WEBAPP D-Link DIR-816 form2systime.cgi command injection attempt	CVE-2018-17066	Web Services and Applications	2
SERVER-WEBAPP D-Link DIR-816 syslogIp command injection attempt	CVE-2018-17064	Web Services and Applications	2
SERVER-WEBAPP D-Link DNS-320 ShareCenter command injection attempt	CVE-2019-16057	Apache HTTP Server	2
SERVER-WEBAPP D-Link DNS-320 ShareCenter command injection attempt	CVE-2019-16057	Web Services and Applications	2
SERVER-WEBAPP D-Link DNS-326 check_login command injection attempt		Web Services and Applications	1
SERVER-WEBAPP D-Link Multiple Products hedwig.cgi cookie buffer overflow attempt		Web Services and Applications	1
SERVER-WEBAPP D-Link		Web Services	1

Multiple Products info.cgi request buffer overflow attempt		and Applications	
SERVER-WEBAPP D-Link hedwig.cgi NTP service configuration command injection attempt		Web Services and Applications	1
SERVER-WEBAPP D-Link hedwig.cgi directory traversal attempt		Web Services and Applications	2
SERVER-WEBAPP D-Link multiple products ping.ccp command injection attempt	CVE-2015-1187	Web Services and Applications	1
SERVER-WEBAPP D-Link router stack based buffer overflow attempt		Web Services and Applications	1
SERVER-WEBAPP D-Link soap.cgi service command injection attempt		Web Services and Applications	1
SERVER-WEBAPP Dell EMC VMAX CVE-2018-1216 Virtual Appliance Manager Authentication Bypass (Decrypted Traffic)	CVE-2018-1216	Web Services and Applications	2
SERVER-WEBAPP Dell EMC VMAX CVE-2018-1216 Virtual Appliance Manager Authentication Bypass	CVE-2018-1216	Web Services and Applications	2
SERVER-WEBAPP Dell EMC VMAX Virtual Appliance Manager	CVE-2018-1215	Web Services and	1

Directory Traversal (Decrypted Traffic)		Applications	
SERVER-WEBAPP Dell SonicWall GMS set_dns XMLRPC method command injection attempt		Web Services and Applications	1
SERVER-WEBAPP Dell SonicWall GMS set_time_config XMLRPC Method Command Injection Attempt	CVE-2018-9866	Web Services and Applications	1
SERVER-WEBAPP Dell Storage Manager EmWebsiteServlet Directory Traversal (Decrypted Traffic)	CVE-2017-10949	Web Services and Applications	3
SERVER-WEBAPP Digium Asterisk CVE-2018-7287 WebSocket Frame Empty Payload Denial of Service	CVE-2018-7287	Web Services and Applications	4
SERVER-WEBAPP Digium Asterisk CVE-2018-7287 WebSocket Frame Empty Payload Denial of Service	CVE-2018-7287	Web Services and Applications	3
SERVER-WEBAPP Drupal Core Form Rendering Remote Code Execution CVE-2018-7602	CVE-2018-7602	Web Services and Applications	1
SERVER-WEBAPP Drupal Core Form Rendering Remote Code Execution	CVE-2018-7600	Web Services and Applications	2

SERVER-WEBAPP Drupal Core Web Services CVE-2019-6340 Remote Code Execution	CVE-2019-6340	Web Services and Applications	3
SERVER-WEBAPP Drupal Core file_create_filename Stored Cross-Site Scripting	CVE-2019-6341	Web Services and Applications	2
SERVER-WEBAPP Drupal Core phar Stream Wrapper Insecure Deserialization	CVE-2019-6339	Web Services and Applications	2
SERVER-WEBAPP Drupal Unsafe Internal Attribute Remote Code Execution Attempt	CVE-2018-7600	Web Services and Applications	1
SERVER-WEBAPP EMC VMAX3 CVE-2017-4997 VASA Provider UploadConfigurator Directory Traversal I	CVE-2017-4997	Web Services and Applications	2
SERVER-WEBAPP EMC VMAX3 CVE-2017-4997 VASA Provider UploadConfigurator Directory Traversal II	CVE-2017-4997	Web Services and Applications	2
SERVER-WEBAPP EMC VMAX3 VASA Provider UploadConfigurator Directory Traversal (Decrypted Traffic)	CVE-2017-4997	Web Services and Applications	1
SERVER-WEBAPP EventManager page.php sql injection	CVE-2018-6576	Web Services and Applications	1

attempt SQL injection attempt			
SERVER-WEBAPP GE MDS PulseNET CVE-2018-10611 Remote Invocation Insecure Deserialization	CVE-2018-10611	Web Services and Applications	3
SERVER-WEBAPP GIT CVE-2018-11235 Submodules Directory Traversal I	CVE-2018-11235	Web Services and Applications	3
SERVER-WEBAPP GIT CVE-2018-11235 Submodules Directory Traversal II	CVE-2018-11235	Web Services and Applications	3
SERVER-WEBAPP GPON Router Authentication Bypass And Command Injection attempt	CVE-2018-10562	Web Services and Applications	1
SERVER-WEBAPP GPON Router authentication bypass and command injection attempt	CVE-2018-10562	Web Services and Applications	1
SERVER-WEBAPP HP Data Protector FinishedCopy SQL Injection attempt	CVE-2011-3162	Web Services and Applications	1
SERVER-WEBAPP HP Data Protector GetPolicies SQL Injection attempt	CVE-2011-3157	Web Services and Applications	1
SERVER-WEBAPP HP Data Protector LogClientInstallation	CVE-2011-3156	Web Services and Applications	1

SQL Injection attempt			
SERVER-WEBAPP HP Data Protector Multiple Products FinishedCopy SQL Injection	CVE-2011-3162	Web Services and Applications	1
SERVER-WEBAPP HP Data Protector Multiple Products GetPolicies SQL Injection	CVE-2011-3157	Web Services and Applications	1
SERVER-WEBAPP HP Data Protector Multiple Products GetPolicies SQL Injection	CVE-2011-3157	Web Services and Applications	4
SERVER-WEBAPP HP Data Protector Multiple Products LogClientInstallation SQL Injection	CVE-2011-3156	Web Services and Applications	1
SERVER-WEBAPP HP Data Protector Multiple Products RequestCopy SQL Injection	CVE-2011-3158	Web Services and Applications	1
SERVER-WEBAPP HP Data Protector Multiple Products RequestCopy SQL Injection	CVE-2011-3158	Web Services and Applications	4
SERVER-WEBAPP HP Enterprise Vertica validateAdminConfig Remote Command Injection	CVE-2016-2002	Web Services and Applications	1
SERVER-WEBAPP HP Enterprise Vertica validateAdminConfig command injection	CVE-2016-2002	Web Services and Applications	1

attempt			
SERVER-WEBAPP HP IMC guiDataDetail Java expression language injection attempt	CVE-2017-12523	Web Services and Applications	1
SERVER-WEBAPP HP IMC iccSelectDeviceSeries Java expression language injection attempt	CVE-2017-12510	Web Services and Applications	1
SERVER-WEBAPP HP IMC mediaForAction Java expression language injection attempt	CVE-2017-12494	Web Services and Applications	1
SERVER-WEBAPP HP IMC mibBrowser arbitrary Java object deserialization attempt	CVE-2017-12556	Web Services and Applications	1
SERVER-WEBAPP HP IMC operatorGroupSelectContent Java expression language injection attempt	CVE-2017-12524	Web Services and Applications	1
SERVER-WEBAPP HP IMC userSelectPagingContent Java expression language injection attempt	CVE-2017-12521	Web Services and Applications	2
SERVER-WEBAPP HP IMC wmiConfigContent Java expression language injection	CVE-2017-12526	Web Services and Applications	1

attempt			
SERVER-WEBAPP HP Intelligent Management Center DeviceService Java expression language injection attempt	CVE-2017-12491	Web Services and Applications	1
SERVER-WEBAPP HP Intelligent Management Center dbman Buffer Overflow		Web Services and Applications	1
SERVER-WEBAPP HP Intelligent Management Center img Buffer Overflow		Web Services and Applications	1
SERVER-WEBAPP HP Moonshot Provisioning Manager Appliance khuploadfile.cgi directory traversal attempt	CVE-2017-8975	Web Services and Applications	2
SERVER-WEBAPP HP Network Automation RedirectServlet SQL injection attempt	CVE-2017-5810	Web Services and Applications	1
SERVER-WEBAPP HP OpenView CGI parameter buffer overflow attempt	CVE-2010-1551	Web Services and Applications	1
SERVER-WEBAPP HP OpenView NNM getnnmdata.exe CGI ICount parameter buffer overflow attempt	CVE-2010-1554	Web Services and Applications	1

SERVER-WEBAPP HP OpenView NNM getnnmdata.exe CGI MaxAge parameter buffer overflow attempt	CVE-2010-1553	Web Services and Applications	1
SERVER-WEBAPP HP OpenView NNM jovgraph.exe CGI hostname parameter bugger overflow attempt	CVE-2010-1555	Web Services and Applications	1
SERVER-WEBAPP HP OpenView NNM nnmRptConfig.exe CGI Host parameter buffer overflow attempt	CVE-2009-3848	Web Services and Applications	1
SERVER-WEBAPP HP OpenView NNM ovlogin.exe CGI Host parameter buffer overflow attempt	CVE-2009-4180	Web Services and Applications	1
SERVER-WEBAPP HP OpenView NNM ovlogin.exe passwd parameter buffer overflow attempt	CVE-2009-3846	Web Services and Applications	1
SERVER-WEBAPP HP OpenView NNM ovlogin.exe userid parameter buffer overflow attempt	CVE-2009-3846	Web Services and Applications	1
SERVER-WEBAPP HP OpenView NNM ovutil.dll getProxiedStorageAddress buffer overflow	CVE-2010-1961	Web Services and Applications	1

attempt			
SERVER-WEBAPP HP OpenView NNM snmp.exe CGI Host parameter buffer overflow attempt	CVE-2009-3849	Web Services and Applications	1
SERVER-WEBAPP HP OpenView NNM webappmon.exe buffer overflow attempt	CVE-2010-2703	Web Services and Applications	1
SERVER-WEBAPP HP OpenView Network Node Manager OpenView5 CGI buffer overflow attempt	CVE-2008-0067	Web Services and Applications	1
SERVER-WEBAPP HP OpenView Network Node Manager URI rping stack buffer overflow attempt	CVE-2009-1420	Web Services and Applications	1
SERVER-WEBAPP HP OpenView Network Node Manager nnmRptConfig.exe Template format string code execution attempt	CVE-2011-0270	Web Services and Applications	1
SERVER-WEBAPP HP OpenView Network Node Manager nnmRptConfig.exe multiple parameters buffer overflow attempt	CVE-2011-0265	Web Services and Applications	1
SERVER-WEBAPP HP OpenView Network Node Manager ovalarm.exe Accept-	CVE-2009-4179	Web Services and Applications	1

Language buffer overflow attempt			
SERVER-WEBAPP HP OpenView Network Node Manager ovwebsnmpsrv.exe OVwSelection buffer overflow attempt - GET	CVE-2009-4181	Web Services and Applications	1
SERVER-WEBAPP HP OpenView Network Node Manager ovwebsnmpsrv.exe OVwSelection buffer overflow attempt - POST	CVE-2009-4181	Web Services and Applications	1
SERVER-WEBAPP HP OpenView Network Node Manager ovwebsnmpsrv.exe displayWidth buffer overflow attempt - GET	CVE-2011-0262	Web Services and Applications	1
SERVER-WEBAPP HP OpenView Network Node Manager ovwebsnmpsrv.exe displayWidth buffer overflow attempt - POST	CVE-2011-0262	Web Services and Applications	1
SERVER-WEBAPP HP OpenView Network Node Manager rping Stack Buffer Overflow	CVE-2009-1420	Web Services and Applications	2
SERVER-WEBAPP HP OpenView Network Node Manager webappmon.exe host header buffer overflow	CVE-2009-4177	Web Services and Applications	1

attempt			
SERVER-WEBAPP HP OpenView Operations Agent buffer overflow attempt	CVE-2012-2019	Web Services and Applications	1
SERVER-WEBAPP HP OpenView Operations Agent request attempt	CVE-2012-2019	Web Services and Applications	4
SERVER-WEBAPP HP OpenView Performance Insight Server backdoor account code execution attempt	CVE-2011-0276	Web Services and Applications	1
SERVER-WEBAPP HP OpenView Storage Data Protector buffer overflow attempt	CVE-2011-1865	Web Services and Applications	1
SERVER-WEBAPP HP OpenView Storage Data Protector get file buffer overflow attempt	CVE-2011-1729	Web Services and Applications	1
SERVER-WEBAPP HP Openview Network Node Manager OvAcceptLang overflow attempt	CVE-2009-0921	Web Services and Applications	1
SERVER-WEBAPP HP Openview OvWebHelp.exe buffer overflow	CVE-2009-4178	Web Services and Applications	1
SERVER-WEBAPP HP Power Manager formExportDataLogs buffer overflow attempt	CVE-2009-3999	Web Services and Applications	1

SERVER-WEBAPP HP Power Manager remote code execution attempt	CVE-2009-2685	Web Services and Applications	1
SERVER-WEBAPP HP ProCurve Manager CVE-2013-4811 SNAC UpdateDomainControllerServlet Code Execution II	CVE-2013-4811	Web Services and Applications	1
SERVER-WEBAPP HP ProCurve Manager CVE-2013-4811 SNAC UpdateDomainControllerServlet Code Execution III	CVE-2013-4811	Web Services and Applications	1
SERVER-WEBAPP HP ProCurve Manager CVE-2013-4811 SNAC UpdateDomainControllerServlet Code Execution	CVE-2013-4811	Web Services and Applications	1
SERVER-WEBAPP HP SiteScope soap request code execution attempt	CVE-2013-2367	Web Services and Applications	1
SERVER-WEBAPP HP iNode Management Center iNodeMngChecker.exe CVE-2011-1867 Buffer Overflow	CVE-2011-1867	Web Services and Applications	2
SERVER-WEBAPP HP openview network node manager ovlogin.exe buffer overflow - password parameter	CVE-2009-4176	Web Services and Applications	1
SERVER-WEBAPP HP	CVE-2009-	Web Services	1

openview network node manager ovlogin.exe buffer overflow - userid parameter	4176	and Applications	
SERVER-WEBAPP HPE IMC CustomReportTemplate SelectBean Expression Language Injection	CVE-2019-5373	Web Services and Applications	1
SERVER-WEBAPP HPE IMC ForwardRedirect Expression Language Injection		Web Services and Applications	2
SERVER-WEBAPP HPE IMC OperatorGroupTreeSelectBean Expression Language Injection	CVE-2019-5374	Web Services and Applications	1
SERVER-WEBAPP HPE IMC TvxlanLegendBean Expression Language Injection		Web Services and Applications	1
SERVER-WEBAPP HPE IMC deploySelectBootrom Expression Language Injection		Web Services and Applications	3
SERVER-WEBAPP HPE IMC devGroupSelect Expression Language Injection		Web Services and Applications	2
SERVER-WEBAPP HPE IMC sshConfig Expression Language Injection		Web Services and Applications	2

SERVER-WEBAPP HPE Intelligent Management CVE-2017-12490 Center getSelInsBean Expression Language Injection	CVE-2017-12490	Web Services and Applications	2
SERVER-WEBAPP HPE Intelligent Management Center AMF3 Externalizable Deserialization	CVE-2019-11944	Web Services and Applications	1
SERVER-WEBAPP HPE Intelligent Management Center AccessMgrServlet className Insecure Deserialization	CVE-2019-11945	Web Services and Applications	2
SERVER-WEBAPP HPE Intelligent Management Center ByteMessageResource Insecure Deserialization	CVE-2019-11956	Web Services and Applications	2
SERVER-WEBAPP HPE Intelligent Management Center CVE-2017-12558 WebDMServlet Insecure Deserialization	CVE-2017-12558	Web Services and Applications	1
SERVER-WEBAPP HPE Intelligent Management Center CVE-2017-12559 mibFileServlet file Directory Traversal	CVE-2017-12559	Web Services and Applications	2
SERVER-WEBAPP HPE Intelligent Management Center CommonUtils ZIP Directory Traversal	CVE-2017-5793	Web Services and Applications	2

SERVER-WEBAPP HPE Intelligent Management Center FileDownloadServlet fileName Directory Traversal	CVE-2017-5795	Web Services and Applications	2
SERVER-WEBAPP HPE Intelligent Management Center FileUploadServlet Directory Traversal	CVE-2017-5794	Web Services and Applications	2
SERVER-WEBAPP HPE Intelligent Management Center IccSelectDevTypeBean Expression Language Injection	CVE-2019-11941	Web Services and Applications	1
SERVER-WEBAPP HPE Intelligent Management Center PlatNavigationToBean URL Expression Language Injection	CVE-2019-5387	Web Services and Applications	1
SERVER-WEBAPP HPE Intelligent Management Center Platform /rptviewer/servlets/redirectviewer directory traversal attempt	CVE-2017-8983	Web Services and Applications	2
SERVER-WEBAPP HPE Intelligent Management Center RMI Registry Insecure Deserialization	CVE-2017-5792	Web Services and Applications	1
SERVER-WEBAPP HPE Intelligent Management Center SoapConfigBean Expression Language	CVE-2019-11943	Web Services and Applications	1

Injection			
SERVER-WEBAPP HPE Intelligent Management Center TopoMsgServlet className Expression Language Injection	CVE-2019-11942	Web Services and Applications	1
SERVER-WEBAPP HPE Intelligent Management Center ViewBatchTaskResultDetailBean Language Injection	CVE-2019-5386	Web Services and Applications	2
SERVER-WEBAPP HPE Intelligent Management Center WebDMServlet Insecure Deserialization	CVE-2017-12558	Web Services and Applications	1
SERVER-WEBAPP HPE Intelligent Management Center dbman Opcode 10003 Filename Denial of Service	CVE-2019-5355	Web Services and Applications	1
SERVER-WEBAPP HPE Intelligent Management Center dbman Stack Buffer Overflow	CVE-2017-8956	Web Services and Applications	2
SERVER-WEBAPP HPE Intelligent Management Center getSelInsBean Expression Language Injection	CVE-2017-12490	Web Services and Applications	2
SERVER-WEBAPP HPE Intelligent Management Center ictExpertDownload Expression Language	CVE-2017-12500	Web Services and Applications	2

Injection			
SERVER-WEBAPP HPE Intelligent Management Center imcwlandm Stack Buffer Overflow	CVE-2017-5804	Web Services and Applications	2
SERVER-WEBAPP HPE Intelligent Management Center imcwlandm UserName Stack Buffer Overflow	CVE-2017-5805	Web Services and Applications	2
SERVER-WEBAPP HPE Intelligent Management Center opcode denial-of-service attempt	CVE-2018-7123	Web Services and Applications	3
SERVER-WEBAPP HPE Intelligent Management Center perfAccessMgrServlet Insecure Deserialization	CVE-2017-8962	Web Services and Applications	1
SERVER-WEBAPP HPE Intelligent Management Center perfSelectTask Expression Language Injection	CVE-2019-5385	Web Services and Applications	2
SERVER-WEBAPP HPE Intelligent Management Center userSelectPagingContent Expression Language Injection	CVE-2017-12521	Web Services and Applications	2
SERVER-WEBAPP HPE Moonshot CVE-2017-8977 Provisioning Manager Appliance server_response	CVE-2017-8977	Web Services and Applications	2

Directory Traversal			
SERVER-WEBAPP HPE Moonshot Provisioning Manager Appliance khuploadfile.cgi Directory Traversal (Decrypted Traffic)	CVE-2017-8976	Web Services and Applications	2
SERVER-WEBAPP HPE Network 2017-5811 Automation FileServlet Information Disclosure I	CVE-2017-5811	Web Services and Applications	1
SERVER-WEBAPP HPE Network 2017-5811 Automation FileServlet Information Disclosure II	CVE-2017-5811	Web Services and Applications	1
SERVER-WEBAPP HPE Network Automation CVE-2017-5810 RedirectServlet SQL Injection	CVE-2017-5810	Web Services and Applications	2
SERVER-WEBAPP HPE Network Automation PermissionFilter Authentication Bypass (Decrypted Traffic)	CVE-2017-5812	Web Services and Applications	3
SERVER-WEBAPP HPE Network Automation RedirectServlet SQL Injection (Decrypted Traffic)	CVE-2017-5810	Web Services and Applications	2
SERVER-WEBAPP HPE Network CVE-2017-5812 Automation PermissionFilter	CVE-2017-5812	Web Services and Applications	3

Authentication Bypass			
SERVER-WEBAPP HPE Operations Orchestration CVE-2017-8994 central-remoting Insecure Deserialization	CVE-2017-8994	Web Services and Applications	2
SERVER-WEBAPP HPE System Management Homepage buffer overflow attempt	CVE-2016-4395	Web Services and Applications	2
SERVER-WEBAPP HPE System Management Homepage cross site scripting attempt	CVE-2017-12544	Web Services and Applications	1
SERVER-WEBAPP Hewlett Packard Enterprise Vertica validateAdminConfig Remote Command Injection (Decrypted Traffic)	CVE-2016-2002	Web Services and Applications	1
SERVER-WEBAPP Horde Groupware Webmail data import PHP code injection attempt	CVE-2020-8518	Web Services and Applications	1
SERVER-WEBAPP Horde Groupware Webmail data import PHP code injection attempt	CVE-2020-8518	Web Services and Applications	3
SERVER-WEBAPP Hp OpenView CGI parameter buffer overflow attempt	CVE-2011-3166	Web Services and Applications	1

SERVER-WEBAPP IBM Informix Dynamic Server index.php testconn Heap Buffer Overflow	CVE-2017-1092	Web Services and Applications	1
SERVER-WEBAPP IBM Informix OpenAdmin Tool welcomeService.php Command Execution	CVE-2017-1092	Web Services and Applications	3
SERVER-WEBAPP IBM OpenAdmin Tool SOAP welcomeService.php PHP code injection attempt	CVE-2017-1092	Web Services and Applications	1
SERVER-WEBAPP IBM QRadar SIEM CVE-2018-1418 command injection attempt	CVE-2018-1418	Web Services and Applications	3
SERVER-WEBAPP IBM Spectrum Protect Plus CVE-2020-4241 Command Injection Attempt (Encrypted Traffic)	CVE-2020-4241	Web Services and Applications	1
SERVER-WEBAPP IBM Spectrum Protect Plus CVE-2020-4241 Command Injection Attempt	CVE-2020-4241	Web Services and Applications	1
SERVER-WEBAPP IBM Spectrum Protect Plus hfpackage CVE-2020-4212 Command Injection (Decrypted Traffic)	CVE-2020-4212	Web Services and Applications	1

SERVER-WEBAPP IBM Spectrum Protect Plus hfpackage CVE-2020-4212 Command Injection	CVE-2020-4212	Web Services and Applications	1
SERVER-WEBAPP IBM Spectrum Protect Plus hostname CVE-2020-4211 Command Injection	CVE-2020-4211	Web Services and Applications	1
SERVER-WEBAPP IBM WebSphere Application Server remote code execution attempt	CVE-2019-4279	Web Services and Applications	2
SERVER-WEBAPP Joomla 3.7.0 com_fields view SQL injection attempt	CVE-2017-8917	Web Services and Applications	1
SERVER-WEBAPP Joomla 3.7.0 com_fields view SQL injection attempt	CVE-2017-8917	Web Services and Applications	2
SERVER-WEBAPP Joomla Aist id SQL Injection	CVE-2018-5993	Web Services and Applications	2
SERVER-WEBAPP Joomla CW Articles Attachments SQL injection attempt	CVE-2018-14592	Web Services and Applications	2
SERVER-WEBAPP Joomla CW Tags Searchtext SQL injection attempt	CVE-2018-7313	Web Services and Applications	2
SERVER-WEBAPP	CVE-2018-	Web Services	1

Joomla CheckList Extension SQL Injection	7318	and Applications	
SERVER-WEBAPP Joomla Component Collection Factory SQL injection attempt	CVE-2018-17383	Web Services and Applications	2
SERVER-WEBAPP Joomla Component JMS Music 1.1.1 SQL injection attempt	CVE-2018-6581	Web Services and Applications	1
SERVER-WEBAPP Joomla Component Swap Factory SQL injection attempt	CVE-2018-17384	Web Services and Applications	2
SERVER-WEBAPP Joomla DT Register SQL injection attempt CVE-2018-6584	CVE-2018-6584	Web Services and Applications	1
SERVER-WEBAPP Joomla Gridbox app Cross Site Scripting	CVE-2018-11690	Web Services and Applications	1
SERVER-WEBAPP Joomla JE PayperVideo extension SQL injection attempt	CVE-2018-6578	Web Services and Applications	1
SERVER-WEBAPP Joomla JEXTN Membership extension SQL injection attempt	CVE-2018-6577	Web Services and Applications	1
SERVER-WEBAPP Joomla JEXTN Reverse Auction extension SQL injection attempt	CVE-2018-6579	Web Services and Applications	1

SERVER-WEBAPP Joomla Jimtawl id parameter SQL injection attempt	CVE-2018-17399	Web Services and Applications	1
SERVER-WEBAPP Joomla PostInstall Message SQL injection attempt CVE-2018-6376	CVE-2018-6376	Web Services and Applications	2
SERVER-WEBAPP Joomla ProjectLog search SQL injection attempt	CVE-2018-6024	Web Services and Applications	1
SERVER-WEBAPP Joomla ProjectLog search SQL injection attempt	CVE-2018-6024	Web Services and Applications	2
SERVER-WEBAPP Joomla Saxum Astro Component SQL injection attempt	CVE-2018-7180	Web Services and Applications	1
SERVER-WEBAPP Joomla Saxum Astro Component SQL injection attempt	CVE-2018-7180	Web Services and Applications	2
SERVER-WEBAPP Joomla Saxum Picker SQL injection attempt CVE-2018-7178	CVE-2018-7178	Web Services and Applications	2
SERVER-WEBAPP Joomla Saxum Picker SQL injection attempt	CVE-2018-7178	Web Services and Applications	1
SERVER-WEBAPP Joomla com_realestatemanager		Web Services and Applications	1

module SQL injection attempt			
SERVER-WEBAPP Joomla component Alexandria Book Library SQL injection attempt	CVE-2018-7312	Web Services and Applications	2
SERVER-WEBAPP Joomla component AlphaIndex Dictionaries SQL injection attempt	CVE-2018-17397	Web Services and Applications	2
SERVER-WEBAPP Joomla component Jimtawl 2.2.5 arbitrary PHP file upload attempt	CVE-2018-6580	Web Services and Applications	1
SERVER-WEBAPP Joomla component Reverse Auction Factory SQL injection attempt	CVE-2018-17376	Web Services and Applications	2
SERVER-WEBAPP Joomla component Timetable Schedule 3.6.8 SQL injection attempt	CVE-2018-17394	Web Services and Applications	2
SERVER-WEBAPP Joomla jextn-classifieds SQL injection attempt	CVE-2018-6575	Web Services and Applications	1
SERVER-WEBAPP Joomla! CMS CVE-2018-8045 User Notes List View SQL Injection	CVE-2018-8045	Web Services and Applications	2
SERVER-WEBAPP Joomla! com_fields SQL Injection	CVE-2017-8917	Web Services and Applications	2

SERVER-WEBAPP Kaspersky Anti-Virus directory traversal attempt	CVE-2017-9812	Web Services and Applications	2
SERVER-WEBAPP Kaspersky Linux File Server WMC cross site scripting attempt	CVE-2017-9813	Web Services and Applications	3
SERVER-WEBAPP Kaspersky Linux File Server WMC directory traversal attempt	CVE-2017-9812	Web Services and Applications	2
SERVER-WEBAPP Kibana Console for Elasticsearch local file inclusion attempt	CVE-2018-17246	Other Web Server	2
SERVER-WEBAPP KingComposer Plugin For WordPress CVE-2020-15299 XSS	CVE-2020-15299	Web Services and Applications	1
SERVER-WEBAPP Linksys E series denial of service attempt		Web Services and Applications	2
SERVER-WEBAPP Linksys E-Series apply.cgi Cross Site Scripting Attempt		Web Services and Applications	1
SERVER-WEBAPP Linksys E-Series apply.cgi directory traversal attempt		Web Services and Applications	2
SERVER-WEBAPP Linksys E1500/E2500 apply.cgi submit_button		Web Services and Applications	1

page redirection attempt			
SERVER-WEBAPP Linksys WRT120N tmUnblock.cgi TM_Block_URL parameter fprintf stack buffer overflow attempt		Web Services and Applications	1
SERVER-WEBAPP Linksys WVBR0-25 Wireless Video Bridge command injection attempt	CVE-2017-17411	Web Services and Applications	1
SERVER-WEBAPP ManageEngine Applications Manager Apache Commons Collections Insecure Deserialization	CVE-2016-9498	Web Services and Applications	1
SERVER-WEBAPP ManageEngine Applications Manager MenuHandlerServlet SQL Injection	CVE-2016-9488	Web Services and Applications	1
SERVER-WEBAPP ManageEngine Applications Manager mypage.do SQL injection attempt	CVE-2017-16849	Web Services and Applications	2
SERVER-WEBAPP ManageEngine Applications Manager showActionProfiles.do SQL injection attempt	CVE-2017-16850	Web Services and Applications	2
SERVER-WEBAPP ManageEngine	CVE-2017-	Web Services and	2

Applications Manager showresource.do SQL injection attempt	16847	Applications	
SERVER-WEBAPP ManageEngine Applications Manager testCredential.do command injection attempt	CVE-2018-7890	Web Services and Applications	1
SERVER-WEBAPP ManageEngine Desktop Central FileUploadServlet directory traversal attempt	CVE-2015-8249	Web Services and Applications	2
SERVER-WEBAPP ManageEngine Desktop Central MSP StatusUpdateServlet directory traversal attempt	CVE-2014-9404	Web Services and Applications	2
SERVER-WEBAPP ManageEngine Multiple Products directory traversal attempt	CVE-2014-5301	Web Services and Applications	2
SERVER-WEBAPP ManageEngine NetFlow Analyzer DisplayChartPDF directory traversal attempt	CVE-2014-5446	Web Services and Applications	3
SERVER-WEBAPP ManageEngine ServiceDesk ExportImport.do directory traversal attempt		Web Services and Applications	2

SERVER-WEBAPP ManageEngine ServiceDesk FileDownload.jsp fName directory traversal attempt		Web Services and Applications	2
SERVER-WEBAPP ManageEngine ServiceDesk Plus FileUploader servlet directory traversal attempt		Web Services and Applications	2
SERVER-WEBAPP Micro Focus Secure Messaging Gateway enginelist.php SQL Injection CVE-2018-12464	CVE-2018-12464	Web Services and Applications	1
SERVER-WEBAPP Microsoft SharePoint BdcAdminService remote code execution attempt	CVE-2019-1295	Web Services and Applications	1
SERVER-WEBAPP Microsoft SharePoint CVE-2019-1443 Information Disclosure	CVE-2019-1443	Web Services and Applications	1
SERVER-WEBAPP Microsoft Sharepoint machineKey information disclosure attempt	CVE-2020-17061	Web Services and Applications	1
SERVER-WEBAPP Mitsubishi Electric CVE-2017-9638 E-Designer SetupAlarm Font Stack Buffer Overflow	CVE-2017-9638	Web Services and Applications	3

SERVER-WEBAPP Mitsubishi Electric CVE-2017-9638 E-Designer SetupAlarm Font Stack Buffer Overflow	CVE-2017-9638	Web Services and Applications	4
SERVER-WEBAPP Mitsubishi Electric E-Designer BEComliSlave Status_bit Stack Buffer Overflow	CVE-2017-9638	Web Services and Applications	4
SERVER-WEBAPP Nagios XI Autodiscovery CVE-2019-9164 Job Command Injection	CVE-2019-9164	Web Services and Applications	2
SERVER-WEBAPP Nagios XI CVE-2018-8734 SQL injection attempt	CVE-2018-8734	Web Services and Applications	1
SERVER-WEBAPP Nagios XI CVE-2018-8734 command injection attempt	CVE-2018-8734	Web Services and Applications	1
SERVER-WEBAPP Nagios XI CVE-2018-8734 database settings modification attempt	CVE-2018-8734	Web Services and Applications	1
SERVER-WEBAPP Nagios XI Cmdsubsys Command Injection	CVE-2018-15709	Web Services and Applications	2
SERVER-WEBAPP Nagios XI Magpie cURL Argument Injection	CVE-2018-15708	Web Services and Applications	2
SERVER-WEBAPP Nagios XI SNMP Trap SQL Injection		Web Services and Applications	3

SERVER-WEBAPP Nagios XI alert cloud cross site scripting attempt		Web Services and Applications	2
SERVER-WEBAPP Nagios XI command_test.php Command Injection		Web Services and Applications	2
SERVER-WEBAPP Nagios XI utils-rrdexport.inc.php get_rrd_data Command Injection		Web Services and Applications	2
SERVER-WEBAPP NagiosXI CVE-2018-8734 SQL injection attempt	CVE-2018-8734	Web Services and Applications	1
SERVER-WEBAPP NetGain Systems Enterprise Manager CVE-2017-16598 snmpwalk ip Directory Traversal	CVE-2017-16598	Web Services and Applications	1
SERVER-WEBAPP NetGain Systems Enterprise Manager CVE-2017-16602 exec_jsp Command Execution	CVE-2017-16602	Web Services and Applications	2
SERVER-WEBAPP NetGain Systems Enterprise Manager CVE-2017-17406 RMI Registry Insecure Deserialization	CVE-2017-17406	Web Services and Applications	3
SERVER-WEBAPP NetGain Systems	CVE-2017-16597	Web Services and	2

Enterprise Manager TFtpServer Filename Directory Traversal CVE-2017-16597		Applications	
SERVER-WEBAPP Netgear DGN1000B setup.cgi cross site scripting attempt		Web Services and Applications	2
SERVER-WEBAPP Netgear DGN2200 dnslookup.cgi command injection attempt	CVE-2017-6334	Web Services and Applications	2
SERVER-WEBAPP Netgear DGN2200 ping.cgi command injection attempt	CVE-2017-6077	Web Services and Applications	2
SERVER-WEBAPP Netgear DGN2200B stored cross-site scripting attempt		Web Services and Applications	2
SERVER-WEBAPP Netgear ReadyNAS Surveillance cgi_main command injection attempt	CVE-2016-5679	Web Services and Applications	1
SERVER-WEBAPP Netgear ReadyNAS Surveillance cgi_main stack buffer overflow attempt	CVE-2016-5680	Web Services and Applications	1
SERVER-WEBAPP Netgear ReadyNAS Surveillance cgi_system command injection attempt		Web Services and Applications	1

SERVER-WEBAPP Netgear ReadyNAS Surveillance debugging_center_utils command injection attempt	CVE-2016-5674	Web Services and Applications	1
SERVER-WEBAPP Netgear ReadyNAS Surveillance handle_daylightsaving command injection attempt	CVE-2016-5675	Web Services and Applications	1
SERVER-WEBAPP Netgear WNR2000 authentication bypass attempt	CVE-2016-10176	Web Services and Applications	2
SERVER-WEBAPP Netgear WNR2000 hidden_lang_avi stack buffer overflow attempt	CVE-2016-10174	Web Services and Applications	2
SERVER-WEBAPP Netgear WNR2000 information leak attempt	CVE-2016-10175	Web Services and Applications	2
SERVER-WEBAPP Novell File Reporter Agent CVE-2011-0994 XML Parsing Stack Buffer Overflow	CVE-2011-0994	Web Services and Applications	1
SERVER-WEBAPP Novell File Reporter SRS request heap overflow attempt	CVE-2012-4956	Web Services and Applications	1
SERVER-WEBAPP Novell GroupWise Internet	CVE-2012-0271	Web Services and	1

Agent content-length integer overflow attempt		Applications	
SERVER-WEBAPP Novell GroupWise Messenger nmma.exe login memory corruption attempt		Web Services and Applications	1
SERVER-WEBAPP Novell Groupwise Messenger Parameter Memory Corruption Attempt		Web Services and Applications	3
SERVER-WEBAPP Novell Groupwise Messenger parameter memory corruption attempt		Web Services and Applications	1
SERVER-WEBAPP Novell NetIQ Sentinel Server ReportViewServlet directory traversal attempt directory traversal attempt	CVE-2016-1605	Web Services and Applications	3
SERVER-WEBAPP Novell Service Desk directory traversal attempt	CVE-2016-1593	Web Services and Applications	3
SERVER-WEBAPP Novell ZENworks Asset Management Remote Execution	CVE-2019-7231	Web Services and Applications	1
SERVER-WEBAPP Novell ZENworks Configuration Management CVE-2010-5323 Remote Execution		Web Services and Applications	1
SERVER-WEBAPP Novell ZENworks Configuration	CVE-2015-	Web Services and	1

Management GetStoredResult.class SQL injection attempt	0780	Applications	
SERVER-WEBAPP Novell ZENworks Configuration Management Rtrlet Directory Traversal	CVE-2015-0781	Web Services and Applications	2
SERVER-WEBAPP Novell ZENworks Configuration Management queryid SQL injection attempt	CVE-2015-0782	Web Services and Applications	1
SERVER-WEBAPP Novell ZENworks Configuration Management rtrlet.class directory traversal attempt	CVE-2015-0781	Web Services and Applications	2
SERVER-WEBAPP Novell ZENworks Configuration Management rtrlet.class directory traversal attempt	CVE-2015-0783	Web Services and Applications	2
SERVER-WEBAPP Novell ZENworks Configuration Management rtrlet.class directory traversal attempt	CVE-2015-0785	Web Services and Applications	2
SERVER-WEBAPP Novell ZENworks Configuration Management schedule.ScheduleQuery SQL Injection	CVE-2015-0782	Web Services and Applications	1
SERVER-WEBAPP Novell Zenworks Mobile Management cross site scripting attempt		Web Services and Applications	2

SERVER-WEBAPP OpenMRS Reference Application sessionLocation CVE-2020-5730 Reflected Cross-Site Scripting	CVE-2020-5730	Web Services and Applications	5
SERVER-WEBAPP Oracle Business Intelligence BIRemotingServlet AMF Insecure Deserialization	CVE-2020-2950	Web Services and Applications	1
SERVER-WEBAPP Oracle Business Intelligence and XML Publisher XML external entity injection attempt	CVE-2019-2616	Web Services and Applications	2
SERVER-WEBAPP Oracle Business Intelligence directory traversal attempt	CVE-2019-2588	Web Services and Applications	2
SERVER-WEBAPP Oracle Business Intelligence remote jsp file include attempt	CVE-2019-2771	Web Services and Applications	1
SERVER-WEBAPP Oracle E-Business Suite Advanced Outbound Telephony CVE-2020-2854 Cross-Site Scripting	CVE-2020-2854	Web Services and Applications	1
SERVER-WEBAPP Oracle E-Business Suite Advanced Outbound Telephony CVE-2020-2856 Cross-Site Scripting	CVE-2020-2856	Web Services and Applications	1

SERVER-WEBAPP Oracle E-Business Suite Advanced Outbound Telephony CVE-2020-2871 Cross-Site Scripting	CVE-2020-2871	Web Services and Applications	2
SERVER-WEBAPP Oracle E-Business Suite Advanced Outbound Telephony Calendar CVE-2020-2852 Cross-Site Scripting	CVE-2020-2852	Web Services and Applications	2
SERVER-WEBAPP Oracle E-Business Suite CVE-2019-2633 SQL Injection		Web Services and Applications	2
SERVER-WEBAPP Oracle E-Business Suite General Ledger SQL Injection	CVE-2019-2638	Web Services and Applications	2
SERVER-WEBAPP Oracle E-Business Suite General Ledger SQL Injection	CVE-2019-2638	Web Services and Applications	4
SERVER-WEBAPP Oracle E-Business Suite Human Resources (CVE-2020-2956) SQL Injection	CVE-2020-2956	Web Services and Applications	1
SERVER-WEBAPP Oracle E-Business Suite Human Resources (CVE-2020-2956) SQL Injection	CVE-2020-2956	Web Services and Applications	5
SERVER-WEBAPP Oracle E-Business Suite Human Resources CVE-2020-	CVE-2020-2586	Web Services and Applications	1

2586 SQL Injection			
SERVER-WEBAPP Oracle E-Business Suite Human Resources CVE-2020-2586 SQL Injection	CVE-2020-2586	Web Services and Applications	4
SERVER-WEBAPP Oracle E-Business Suite Human Resources CVE-2020-2587 SQL Injection	CVE-2020-2587	Web Services and Applications	1
SERVER-WEBAPP Oracle E-Business Suite Human Resources CVE-2020-2587 SQL Injection	CVE-2020-2587	Web Services and Applications	4
SERVER-WEBAPP Oracle E-Business Suite Human Resources CVE-2020-2882 SQL Injection	CVE-2020-2882	Web Services and Applications	2
SERVER-WEBAPP Oracle E-Business Suite Human Resources CVE-2020-2882 SQL Injection	CVE-2020-2882	Web Services and Applications	5
SERVER-WEBAPP Oracle Fusion Middleware MapViewer arbitrary JSP file upload attempt	CVE-2017-3230	Web Services and Applications	1
SERVER-WEBAPP Oracle Fusion Middleware MapViewer directory traversal attempt	CVE-2017-3230	Web Services and Applications	1
SERVER-WEBAPP Oracle Identity Manager CVE-2017-10151 Default Credentials I	CVE-2017-10151	Web Services and Applications	1

SERVER-WEBAPP Oracle Identity Manager CVE-2017-10151 Default Credentials II	CVE-2017-10151	Web Services and Applications	3
SERVER-WEBAPP Oracle JDeveloper ADF Faces Untrusted Deserialization	CVE-2019-2904	Web Services and Applications	1
SERVER-WEBAPP Oracle Java Web Server WebDAV Stack Buffer Overflow attempt	CVE-2010-0361	Web Services and Applications	1
SERVER-WEBAPP Oracle Opera Property Management System ProcessInfo command injection attempt	CVE-2016-5563	Web Services and Applications	3
SERVER-WEBAPP Oracle Secure Backup Admin Server command injection attempt	CVE-2011-2261	Web Services and Applications	1
SERVER-WEBAPP Oracle Secure Backup web tool command injection attempt	CVE-2011-2261	Web Services and Applications	1
SERVER-WEBAPP Oracle WebLogic (CVE-2020-14625) Insecure Deserialization	CVE-2020-14625	Web Services and Applications	1
SERVER-WEBAPP Oracle WebLogic CVE-2020-14644 Insecure Deserialization	CVE-2020-14644	Web Services and Applications	1
SERVER-WEBAPP Oracle	CVE-2020-	Web Services	1

WebLogic CVE-2020-2798 Insecure Deserialization	2798	and Applications	
SERVER-WEBAPP Oracle WebLogic CVE-2020-2883 Insecure Deserialization		Web Services and Applications	1
SERVER-WEBAPP Oracle WebLogic CVE-2020-2884 Insecure Deserialization		Web Services and Applications	1
SERVER-WEBAPP Oracle WebLogic CVE-2020-2963 Insecure Deserialization		Web Services and Applications	2
SERVER-WEBAPP Oracle WebLogic Remote Diagnosis Assistant rda_tfa_ref_date Command Injection	CVE-2018-2615	Web Services and Applications	2
SERVER-WEBAPP Oracle WebLogic Server Activator Insecure Deserialization CVE-2018-2893	CVE-2018-2893	Web Services and Applications	1
SERVER-WEBAPP Oracle WebLogic Server CVE-2017-10271 Remote Command Execution	CVE-2017-10271	Web Services and Applications	2
SERVER-WEBAPP Oracle WebLogic Server DeploymentService Directory Traversal	CVE-2019-2618	Web Services and Applications	1
SERVER-WEBAPP Oracle WebLogic Server	CVE-2019-	Web Services and	2

DeploymentService Directory Traversal	2618	Applications	
SERVER-WEBAPP Oracle WebLogic Server arbitrary JSP file upload attempt	CVE-2018-2894	Web Services and Applications	3
SERVER-WEBAPP Oracle WebLogic Server unauthenticated modified JSP access attempt	CVE-2018-2894	Web Services and Applications	1
SERVER-WEBAPP Oracle Weblogic CVE-2019-2647 ForeignRecoveryContext External Entity Injection	CVE-2019-2647	Web Services and Applications	1
SERVER-WEBAPP Oracle Weblogic CVE-2019-2729 Insecure Deserialization	CVE-2019-2729	Web Services and Applications	2
SERVER-WEBAPP Oracle Weblogic EJBTaglibDescriptor External Entity Injection	CVE-2019-2888	Web Services and Applications	1
SERVER-WEBAPP Oracle Weblogic EJBTaglibDescriptor External Entity Injection	CVE-2019-2888	Web Services and Applications	4
SERVER-WEBAPP Oracle Weblogic UnknownMsgHeader External Entity Injection	CVE-2019-2649	Web Services and Applications	2
SERVER-WEBAPP Oracle Weblogic WsrmSequenceContext	CVE-2019-2650	Web Services and	2

External Entity Injection		Applications	
SERVER-WEBAPP Oracle Weblogic WsrmServerPayloadContext External Entity Injection	CVE-2019-2648	Web Services and Applications	2
SERVER-WEBAPP PHP CVE-2017-5340 zend_hash_destroy Uninitialized Pointer Code Execution	CVE-2017-5340	Web Services and Applications	2
SERVER-WEBAPP PHP CVE-2018-7584 http_fopen_wrapper Stack Buffer Overflow	CVE-2018-7584	Web Services and Applications	3
SERVER-WEBAPP PHP CVE-2019-9022 dns_get_record Out of Bounds Read	CVE-2019-9022	Web Services and Applications	1
SERVER-WEBAPP PHP CVE-2019-9022 dns_get_record Out of Bounds Read	CVE-2019-9022	Web Services and Applications	3
SERVER-WEBAPP PHP FPM init_request_info PATH_INFO Buffer Underflow	CVE-2019-11043	Web Services and Applications	1
SERVER-WEBAPP PHP Unserialize Integer Overflow Attempt	CVE-2017-5340	Web Services and Applications	1
SERVER-WEBAPP PHP phar extension remote code execution attempt	CVE-2016-4072	Web Services and Applications	2

SERVER-WEBAPP PHP unserialize function use after free memory corruption vulnerability attempt	CVE-2016-7479	Web Services and Applications	2
SERVER-WEBAPP PHP unserialize var_hash use-after-free attempt	CVE-2016-6290	Web Services and Applications	2
SERVER-WEBAPP PHP zend_hash_destroy Uninitialized Pointer Code Execution (Published Exploit)	CVE-2017-5340	Web Services and Applications	2
SERVER-WEBAPP PHP-Fusion Administration Banner Stored Cross-Site Scripting	CVE-2020-12438	Web Services and Applications	1
SERVER-WEBAPP Palo Alto Networks Firewall router.php XML attribute injection attempt	CVE-2017-15944	Web Services and Applications	2
SERVER-WEBAPP PhpWiki Ploticus plugin command injection attempt	CVE-2014-5519	Web Services and Applications	2
SERVER-WEBAPP Pivotal Spring Data REST PATCH request remote code execution attempt	CVE-2017-8046	Web Services and Applications	1
SERVER-WEBAPP Pulse Secure Guacamole URI Information Disclosure (encrypted Traffic)	CVE-2019-11510	Web Services and Applications	2

SERVER-WEBAPP QNAP NAS authLogin.cgi command injection attempt	CVE-2017-6361	Web Services and Applications	1
SERVER-WEBAPP QNAP NAS userConfig.cgi command injection attempt	CVE-2017-6360	Web Services and Applications	1
SERVER-WEBAPP QNAP NAS utilRequest.cgi command injection attempt	CVE-2017-6359	Web Services and Applications	1
SERVER-WEBAPP QNAP QCenter API set_VM_network Command Injection	CVE-2018-0708	Web Services and Applications	2
SERVER-WEBAPP QNAP QCenter API set_VM_network command injection attempt	CVE-2018-0708	Web Services and Applications	1
SERVER-WEBAPP QNAP QCenter API set_VM_passwd command injection attempt	CVE-2018-0707	Web Services and Applications	1
SERVER-WEBAPP QNAP WTS 4.2.1 command injection attempt		Web Services and Applications	2
SERVER-WEBAPP Quest CVE-2018-11143 DR Series Disk Backup Login.pm Command Injection Attempt	CVE-2018-11143	Web Services and Applications	3

SERVER-WEBAPP Quest CVE-2018-11144 DR Series Disk Backup UsersService.pm Update Method Command Injection Attempt	CVE-2018-11144	Web Services and Applications	3
SERVER-WEBAPP Quest CVE-2018-11145 DR Series Disk Backup UsersService.pm delete method command injection attempt	CVE-2018-11145	Web Services and Applications	3
SERVER-WEBAPP Quest CVE-2018-11146 DR Series Disk Backup UsersService.pm update_pw method command injection attempt	CVE-2018-11146	Web Services and Applications	3
SERVER-WEBAPP Quest CVE-2018-11149 DR Series Disk Backup SchedulesService.pm Command Injection Attempt	CVE-2018-11145	Web Services and Applications	3
SERVER-WEBAPP Quest CVE-2018-11151 DR Series Disk Backup PasswordService.pm command injection attempt	CVE-2018-11145	Web Services and Applications	3
SERVER-WEBAPP Quest CVE-2018-11153 DR Series Disk Backup LicenseService.pm Command Injection Attempt	CVE-2018-11153	Web Services and Applications	3

SERVER-WEBAPP Quest DR Series Disk Backup EmailRelayHostService.pm command injection attempt	CVE-2018-11156	Web Services and Applications	1
SERVER-WEBAPP Quest KACE Systems Management Appliance CVE-2018-11138 download_agent_installer.php Command Injection Attempt	CVE-2018-11138	Web Services and Applications	3
SERVER-WEBAPP Quest KACE Systems Management Appliance download_agent_installer.php command injection attempt	CVE-2018-11138	Web Services and Applications	2
SERVER-WEBAPP Quest NetVault Backup CVE-2017-17652 NVBUBackup Count Method SQL Injection	CVE-2017-17652	Web Services and Applications	1
SERVER-WEBAPP Quest NetVault Backup Multipart CVE-2018-1163 Request checksession Authentication Bypass	CVE-2018-1163	Web Services and Applications	3
SERVER-WEBAPP Quest NetVault Backup Server NVBUBackupOptionSet SQL injection attempt CVE-2017-17653	CVE-2017-17653	Web Services and Applications	2
SERVER-WEBAPP Rank Math Wordpress SEO Plugin updateMeta		Web Services and	1

REST Endpoint Access Control Weakness		Applications	
SERVER-WEBAPP Rank Math Wordpress SEO Plugin updateMeta REST Endpoint Access Control Weakness		Web Services and Applications	2
SERVER-WEBAPP SAP NetWeaver Message Server Memory Corruption	CVE-2013-1592	Web Services and Applications	1
SERVER-WEBAPP SERVER-WEBAPP Novell NetIQ Sentinel Server ReportViewServlet directory traversal attempt directory traversal attempt	CVE-2016-1605	Web Services and Applications	3
SERVER-WEBAPP SQL Server Reporting Services web application remote code execution attempt	CVE-2020-0618	Web Services and Applications	1
SERVER-WEBAPP Samsung SmartThings Hub video-core Camera URL Buffer Overflow	CVE-2018-3903	Web Services and Applications	4
SERVER-WEBAPP Samsung SmartThings Hub video-core Camera URL Replace Code Execution	CVE-2018-3902	Web Services and Applications	4
SERVER-WEBAPP Samsung SmartThings Hub video-core credentials Code	CVE-2018-3875	Web Services and Applications	4

Execution			
SERVER-WEBAPP Samsung SmartThings Hub videoHostUrl Code Execution	CVE-2018-3872	Web Services and Applications	2
SERVER-WEBAPP Secure Backup login.php uname variable based command injection attempt	CVE-2008-5449	Web Services and Applications	1
SERVER-WEBAPP Seowonintech system_config.cgi local file include attempt	CVE-2016-10760	Web Services and Applications	1
SERVER-WEBAPP Seowonintech system_config.cgi local file include attempt	CVE-2016-10760	Web Services and Applications	2
SERVER-WEBAPP SoftNAS StorageCenter snserv.php command injection attempt CVE-2018-14417	CVE-2018-14417	Web Services and Applications	2
SERVER-WEBAPP Solarwinds Virtualization Manager Apache Commons Collections Insecure Deserialization	CVE-2016-3642	Web Services and Applications	1
SERVER-WEBAPP SonicWall Secure Remote Access diagnostics command injection attempt	CVE-2016-9682	Web Services and Applications	1

SERVER-WEBAPP SonicWall Secure Remote Access gencsr command injection attempt		Web Services and Applications	1
SERVER-WEBAPP SonicWall Secure Remote Access sitecustomization command injection attempt		Web Services and Applications	1
SERVER-WEBAPP SonicWall Secure Remote Access viewcert command injection attempt	CVE-2016-9684	Web Services and Applications	1
SERVER-WEBAPP Sophos Web Security Appliance command injection attempt		Web Services and Applications	1
SERVER-WEBAPP Sophos Web Security Appliance command injection attempt	CVE-2016-9553	Web Services and Applications	1
SERVER-WEBAPP Squid Proxy Digest Authentication Denial of Service	CVE-2019-12525	Web Services and Applications	1
SERVER-WEBAPP Squid Proxy URN Response Processing Heap Buffer Overflow	CVE-2019-12526	Other Web Server	1
SERVER-WEBAPP Squid Proxy URN Response Processing Heap Buffer	CVE-2019-12526	Web Services and Applications	1

Overflow			
SERVER-WEBAPP Squid Proxy URN Response Processing Heap Buffer Overflow	CVE-2019-12526	Web Services and Applications	4
SERVER-WEBAPP Squid Proxy cachemgr.cgi Reflected Cross-Site Scripting in user_name parameter	CVE- 2019-13345	Web Services and Applications	1
SERVER-WEBAPP Symantec Messaging Gateway performBackupNow.do command injection attempt	CVE-2017-6326	Web Services and Applications	1
SERVER-WEBAPP Trend Micro Apex One and OfficeScan CVE-2020-8599 Directory Traversal (Decrypted Traffic)	CVE-2020-8599	Web Services and Applications	1
SERVER-WEBAPP Trend Micro Apex One and OfficeScan CVE-2020-8599 Directory Traversal	CVE-2020-8599	Web Services and Applications	1
SERVER-WEBAPP Trend Micro Control Manager CVE-2018-3602 AdHocQuery_Processor GetProductCategory SQL Injection	CVE-2018-3602	Web Services and Applications	2
SERVER-WEBAPP Trend Micro Control Manager ProductTree_RightWindow XML External Entity Processing (Decrypted		Web Services and Applications	3

Traffic)			
SERVER-WEBAPP Trend Micro Control Manager XML External Entity Processing (Decrypted Traffic)		Web Services and Applications	3
SERVER-WEBAPP Trend Micro Control Manager cmdHandlerLicenseManager SQL Injection	CVE-2017-11384	Web Services and Applications	2
SERVER-WEBAPP Trend Micro Control Manager cmdHandlerStatusMonitor SQL Injection	CVE-2017-11385	Web Services and Applications	2
SERVER-WEBAPP Trend Micro Control Manager cmdHandlerTVCSCommander SQL Injection	CVE-2017-11383	Web Services and Applications	2
SERVER-WEBAPP Trend Micro IWSVA DeploymentWizardAction GetClusterInfo Command Injection (Decrypted Traffic)		Web Services and Applications	1
SERVER-WEBAPP Trend Micro IWSVA DomainList TestingADKerberos Command Injection (Decrypted Traffic)		Web Services and Applications	2
SERVER-WEBAPP Trend Micro IWSVA domains Command Injection I		Web Services and Applications	2
SERVER-WEBAPP Trend Micro IWSVA domains		Web Services and	2

Command Injection II		Applications	
SERVER-WEBAPP Trend Micro IWSVA domains Command Injection III		Web Services and Applications	2
SERVER-WEBAPP Trend Micro IWSVA testConfiguration Command Injection (Decrypted Traffic)		Web Services and Applications	2
SERVER-WEBAPP Trend Micro Mobile Security CVE-2017-14078 Enterprise eas_agent_unregister slink_id SQL Injection	CVE-2017-14078	Web Services and Applications	2
SERVER-WEBAPP Trend Micro Mobile Security Enterprise eas_agent_sync_client_info slink_id SQL Injection (Decrypted Traffic)	CVE-2017-14078	Web Services and Applications	1
SERVER-WEBAPP Trend Micro Mobile Security Enterprise eas_agent_sync_client_info slink_id SQL Injection I		Web Services and Applications	2
SERVER-WEBAPP Trend Micro Mobile Security Enterprise eas_agent_sync_client_info slink_id SQL Injection II		Web Services and Applications	2
SERVER-WEBAPP Trend Micro Mobile Security	CVE-2017-	Web Services and	2

Enterprise eas_agent_unregister slink_id SQL Injection (Decrypted Traffic)	14078	Applications	
SERVER-WEBAPP Trend Micro Mobile Security Enterprise get_dep_profile id SQL Injection (Decrypted Traffic)	CVE-2017-14078	Web Services and Applications	1
SERVER-WEBAPP Trend Micro OfficeScan CVE-2017-11394 Proxy.php Command Injection	CVE-2017-11394	Web Services and Applications	2
SERVER-WEBAPP Trend Micro OfficeScan Zip Directory Traversal (Decrypted Traffic)	CVE-2019-18187	Web Services and Applications	4
SERVER-WEBAPP Trend Micro OfficeScan attempt		Web Services and Applications	2
SERVER-WEBAPP Trend Micro SafeSync JSON API ad_sync_now command injection attempt		Web Services and Applications	1
SERVER-WEBAPP Trend Micro SafeSync command injection attempt		Web Services and Applications	1
SERVER-WEBAPP Trend Micro SafeSync for Enterprise ad.pm id Remote Command Execution (Decrypted		Web Services and Applications	1

Traffic)			
SERVER-WEBAPP Trend Micro SafeSync for Enterprise check_nfs_server_status Command Injection (Decrypted Traffic)		Web Services and Applications	2
SERVER-WEBAPP Trend Micro SafeSync for Enterprise deviceTool.pm devid Command Injection (Decrypted Traffic)		Web Services and Applications	1
SERVER-WEBAPP Trend Micro SafeSync for Enterprise license Command Injection (Decrypted Traffic)		Web Services and Applications	2
SERVER-WEBAPP Trend Micro SafeSync for Enterprise restartService Command Injection (Decrypted Traffic)		Web Services and Applications	2
SERVER-WEBAPP Trend Micro SafeSync for Enterprise rollback Command Injection (Decrypted Traffic)		Web Services and Applications	1
SERVER-WEBAPP Trend Micro SafeSync for Enterprise rollback Command Injection (Decrypted Traffic)		Web Services and Applications	2
SERVER-WEBAPP Trend Micro Smart Protection	CVE-2017-	Web Services and	1

Server admin_update_program .php command injection attempt	14094	Applications	
SERVER-WEBAPP Trend Micro Smart Protection Server directory traversal attempt	CVE-2017-14095	Web Services and Applications	2
SERVER-WEBAPP Trend Micro Threat Discovery Appliance admin_sys_time.cgi command injection attempt	CVE-2016-7547	Web Services and Applications	1
SERVER-WEBAPP Trend Micro Virtual Mobile Infrastructure apns_worker.py Command Injection (Decrypted Traffic) (Published Exploit)	CVE-2016-6270	Web Services and Applications	2
SERVER-WEBAPP Trend Micro hotfix_upload.cgi command injection attempt	CVE-2016-5840	Web Services and Applications	1
SERVER-WEBAPP Trend Micro proxy_controller.php Command Injection Attempt	CVE-2017-11394	Web Services and Applications	1
SERVER-WEBAPP Trend Micro proxy_controller.php command injection attempt	CVE-2017-11394	Web Services and Applications	2

SERVER-WEBAPP Trend Micro proxy_controller.php command injection attempt	CVE-2017-11394	Web Services and Applications	2
SERVER-WEBAPP VMTurbo Operations Manager vmtadmin.cgi command injection attempt	CVE-2014-5073	Web Services and Applications	1
SERVER-WEBAPP VMWare NSX SD-WAN Edge command injection attempt	CVE-2018-6961	Web Services and Applications	1
SERVER-WEBAPP Veritas NetBackup Appliance getLicense command injection attempt	CVE-2016-7399	Web Services and Applications	1
SERVER-WEBAPP WIFICAM Wireless IP Camera command injection attempt	CVE-2017-18377	Web Services and Applications	2
SERVER-WEBAPP WP plugin Wechat Broadcast directory traversal attempt	CVE-2018-16283	Web Services and Applications	2
SERVER-WEBAPP WP plugin Wechat Broadcast remote file inclusion attempt	CVE-2018-16283	Web Services and Applications	2
SERVER-WEBAPP Western Digital Arkeia Appliance directory traversal attempt		Web Services and Applications	2

SERVER-WEBAPP Western Digital MyCloud command injection attempt	CVE-2016-10108	Web Services and Applications	1
SERVER-WEBAPP Western Digital MyCloud login_mgr.cgi command injection attempt		Web Services and Applications	2
SERVER-WEBAPP Western Digital MyCloud nas_sharing.cgi command injection attempt		Web Services and Applications	1
SERVER-WEBAPP WordPress 10Web Photo Gallery Plugin CVE-2020-9335 Two Stored Cross-Site Scripting	CVE-2020-9335	Web Services and Applications	3
SERVER-WEBAPP WordPress 10Web Photo Gallery SQL Injection		Web Services and Applications	1
SERVER-WEBAPP WordPress Calculated Fields Form CVE-2020-7228 Cross Site Scripting	CVE-2020-7228	Web Services and Applications	1
SERVER-WEBAPP WordPress Comment Content Filter Remote Code Execution	CVE-2019-9787	Web Services and Applications	2
SERVER-WEBAPP	CVE-2019-	Web Services	2

WordPress Crop Image arbitrary file write attempt	8943	and Applications	
SERVER-WEBAPP WordPress GDPR Cookie Consent Plugin Stored Cross-Site Scripting		Web Services and Applications	1
SERVER-WEBAPP WordPress Google Maps Plugin CVE-2019-10692 SQL Injection		Web Services and Applications	2
SERVER-WEBAPP WordPress Ninja Forms Plugin Remote Code Execution	CVE-2019-10869	Web Services and Applications	2
SERVER-WEBAPP WordPress Ninja Forms nf_async_upload arbitrary PHP file upload attempt	CVE-2016-1209	Web Services and Applications	2
SERVER-WEBAPP WordPress Plugin ThemeREX PHP Code Injection	CVE-2020-10257	Web Services and Applications	1
SERVER-WEBAPP WordPress Print-My-Blog plugin server side request forgery attempt	CVE-2019-11565	Web Services and Applications	2
SERVER-WEBAPP WordPress Rencontre plugin SQL injection attempt	CVE-2019-13413	Web Services and Applications	1
SERVER-WEBAPP WordPress Rencontre plugin SQL injection	CVE-2019-13413	Web Services and	2

attempt		Applications	
SERVER-WEBAPP WordPress Rencontre plugin cross site scripting attempt	CVE-2019-13413	Web Services and Applications	1
SERVER-WEBAPP WordPress Ultimate Form Builder Plugin SQL Injection Attempt	CVE-2017-15919	Web Services and Applications	1
SERVER-WEBAPP WordPress Ultimate Form Builder plugin SQL injection attempt	CVE-2017-15919	Web Services and Applications	1
SERVER-WEBAPP WordPress _wp_attached_file CVE-2019-8942 wp_crop_image Directory Traversal	CVE-2019-8942	Web Services and Applications	2
SERVER-WEBAPP WordPress embedded URL video cross site scripting attempt		Web Services and Applications	2
SERVER-WEBAPP WordPress load-scripts.php Denial of Service	CVE-2018-6389	Web Services and Applications	3
SERVER-WEBAPP WordPress login denial of service attempt		Web Services and Applications	2
SERVER-WEBAPP WordPress meta_input Path Traversal Attempt	CVE-2019-8942	Web Services and Applications	1

SERVER-WEBAPP WordPress plugin Grace Media Player local file inclusion attempt	CVE-2019-9618	Web Services and Applications	1
SERVER-WEBAPP WordPress plugin WP with Spritz remote file include attempt		Web Services and Applications	2
SERVER-WEBAPP Wordpress Excerpt cross site scripting attempt	CVE-2017-5612	Web Services and Applications	3
SERVER-WEBAPP Wordpress Nexos theme SQL injection attempt	CVE-2020-15363	Web Services and Applications	1
SERVER-WEBAPP Wordpress Nexos theme cross site scripting attempt	CVE-2020-15364	Web Services and Applications	1
SERVER-WEBAPP Wordpress NextGEN gallery directory traversal attempt		Web Services and Applications	2
SERVER-WEBAPP Wordpress Scoreme cross site scripting attempt		Web Services and Applications	2
SERVER-WEBAPP Wordpress User History plugin cross site scripting attempt	CVE-2017-15867	Web Services and Applications	2
SERVER-WEBAPP Wordpress image edit	CVE-2019-8942	Web Services and	2

directory traversal attempt		Applications	
SERVER-WEBAPP Wordpress plugin WP with Spritz directory traversal attempt		Web Services and Applications	2
SERVER-WEBAPP Wordpress wp-banners-lite plugin cross site scripting attempt		Web Services and Applications	2
SERVER-WEBAPP Wordpress wpdb prepare sprintf placeholder SQL injection attempt	CVE-2017-14723	Web Services and Applications	2
SERVER-WEBAPP XML entity parsing information disclosure attempt	CVE-2017-7664	Web Services and Applications	1
SERVER-WEBAPP XStream Void CVE-2017-9793 Primitive Denial of Service	CVE-2017-9793	Web Services and Applications	2
SERVER-WEBAPP XStream void primitive denial of service attempt	CVE-2017-9793	Web Services and Applications	2
SERVER-WEBAPP YouPHPTube Encoder getImage.php Command Injection	CVE-2019-5127	Web Services and Applications	1
SERVER-WEBAPP YouPHPTube Encoder getImageMP4.php	CVE-2019-5129	Web Services and Applications	1

Command Injection			
SERVER-WEBAPP Zavio Cam command injection attempt	CVE-2013-2568	Web Services and Applications	1
SERVER-WEBAPP Zeroshell Linux Router command injection attempt	CVE-2019-12725	Web Services and Applications	1
SERVER-WEBAPP Zeroshell Linux Router command injection attempt	CVE-2019-12725	Web Services and Applications	2
SERVER-WEBAPP Zoho ManageEngine Applications Manager AlertRes_Mtrgrp.jsp sid CVE-2020-15533 SQL Injection	CVE-2020-15533	Web Services and Applications	1
SERVER-WEBAPP Zoho ManageEngine Applications Manager CVE-2019-11448 Popup_SLA.jsp sid SQL Injection	CVE-2019-11448	Web Services and Applications	2
SERVER-WEBAPP Zoho ManageEngine Applications Manager FaultTemplateOptions.jsp resourceid SQL Injection	CVE-2019-11469	Web Services and Applications	1
SERVER-WEBAPP Zoho ManageEngine Applications Manager MyPage.do CVE-2020-27995 SQL Injection	CVE-2020-27995	Web Services and Applications	1

SERVER-WEBAPP Zoho ManageEngine CVE-2018-7890 ApplicationManager testCredential.do Command Injection	CVE-2018-7890	Web Services and Applications	2
SERVER-WEBAPP Zoho ManageEngine Desktop Central AppDependency CVE-2020-10859 Arbitrary File Write (Directory Traversal)	CVE-2020-10859	Web Services and Applications	5
SERVER-WEBAPP Zoho ManageEngine NetFlow Analyzer ReportApiHandler compareReport SQL Injection	CVE-2019-12196	Web Services and Applications	2
SERVER-WEBAPP Zoho ManageEngine OpManager APIDBUtil getDevicesForSearchString SQL Injection	CVE-2018-17243	Web Services and Applications	2
SERVER-WEBAPP Zoho ManageEngine OpManager BusinessViewFlashImpl handleBVAction XXE Injection	CVE-2018-18980	Web Services and Applications	2
SERVER-WEBAPP Zoho ManageEngine OpManager FailOverHelperServlet Cross-Site Scripting CVE-2018-12998	CVE-2018-12998	Web Services and Applications	1
SERVER-WEBAPP Zoho ManageEngine	CVE-2018-	Web Services and	2

OpManager OpManagerFailoverUtil customerName SQL Injection CVE-2018-9088	9088	Applications	
SERVER-WEBAPP Zoho ManageEngine OpManager RelationalMailServer addMailServerSettings SQL Injection CVE-2018-18949	CVE-2018-18949	Web Services and Applications	2
SERVER-WEBAPP Zoho ManageEngine OpManager getGraphData SQL Injection	CVE-2018-20173	Web Services and Applications	1
SERVER-WEBAPP Zoho ManageEngine OpManagerDBUtil getProbeNATDetails SQL Injection CVE-2018-9087	CVE-2018-9087	Web Services and Applications	2
SERVER-WEBAPP dnaLIMS viewAppletFsa.cgi directory traversal attempt	CVE-2017-6527	Web Services and Applications	2
SERVER-WEBAPP elFinder PHP connector command injection attempt	CVE-2019-9194	Web Services and Applications	2
SERVER-WEBAPP escan Web Management Console command injection		Web Services and Applications	1

SERVER-WEBAPP iSharer and upRedSun File Sharing Wizard Buffer Overflow	CVE-2019-5129	Web Services and Applications	1
SERVER-WEBAPP multiple vendor calendar application id parameter SQL injection attempt	CVE-2006-3094	Web Services and Applications	3
SERVER-WEBAPP netgear_unauth_exec CVE-2016-1555 command injection	CVE-2016-1555	Web Services and Applications	1
SERVER-WEBAPP newsPHP Language file include attempt		Web Services and Applications	2
SERVER-WEBAPP rConfig ajaxServerSettingsChk.php Command Injection	CVE-2019-16662	Web Services and Applications	1
SERVER-WEBAPP rConfig commands.inc.php CVE-2020-10220 SQL Injection (Decrypted Traffic)	CVE-2020-10220	Web Services and Applications	1
SERVER-WEBAPP rConfig commands.inc.php CVE-2020-10220 SQL Injection (Decrypted Traffic)	CVE-2020-10220	Web Services and Applications	2
SERVER-WEBAPP rConfig commands.inc.php CVE-	CVE-2020-10220	Apache HTTP Server	2

2020-10220 SQL Injection			
SERVER-WEBAPP rConfig commands.inc.php CVE-2020-10220 SQL Injection	CVE-2020-10220	Web Services and Applications	2
SERVER-WEBAPP rConfig commands.inc.php SQL Injection (Decrypted Traffic)	CVE-2020-10220	Web Services and Applications	1
SERVER-WEBAPP rConfig compliancepolicies.inc.php CVE-2020-10546 SQL Injection		Web Services and Applications	2
SERVER-WEBAPP rConfig compliancepolicies.inc.php CVE-2020-10546 SQL Injection	CVE-2020-10546	Web Services and Applications	2
SERVER-WEBAPP rConfig compliancepolicyelements.inc.php CVE-2020-10547 SQL Injection (Decrypted Traffic)	CVE-2020-10547	Web Services and Applications	3
SERVER-WEBAPP rConfig compliancepolicyelements.inc.php CVE-2020-10547 SQL Injection	CVE-2020-10547	Web Services and Applications	3
SERVER-WEBAPP rConfig snippets.inc.php CVE-2020-10549 SQL	CVE-2020-10549	Web Services and	2

Injection		Applications	
SERVER-WEBAPP vBulletin template rendering arbitrary PHP code execution attempt	CVE-2019-16759	Web Services and Applications	1
SERVER-WEBAPP vBulletin updateAvatar PHP Remote Code Execution Attempt	CVE-2019-17132	Web Services and Applications	1
SERVER-WEBAPP wordpress kses bypass cross site scripting attempt	CVE-2015-5714	Web Services and Applications	3
SQL Oracle MySQL Pluggable Auth denial of service attempt	CVE-2017-3599	Database Management System	1

- **Name:** Name of the Signature

- **CVE–ID:** CVE Identification Number - Common Vulnerabilities and Exposures (CVE) provides reference of CVE Identifiers for publicly known information security vulnerabilities.

- **Category:** Class type according to threat

- **Severity:** Degree of severity - The levels of severity are described in the table below:

Severity Level	Severity Criteria
1	Low
2	Moderate
3	High
4	Critical

Important Notice

Sophos Technologies Pvt. Ltd. has supplied this Information believing it to be accurate and reliable at the time of printing, but is presented without warranty of any kind, expressed or implied. Users must take full responsibility for their application of any products. Sophos Technologies Pvt. Ltd. assumes no responsibility for any errors that may appear in this document. Sophos Technologies Pvt. Ltd. reserves the right, without notice to make changes in product design or specifications. Information is subject to change without notice.

RESTRICTED RIGHTS

Corporate Headquarters

Sophos Technologies Pvt. Ltd.

Registered in England and Wales No. 2096520,

The Pentagon, Abingdon Science Park,

Abingdon, OX14 3YP, UK

Web site: www.sophos.com