

SOPHOS

Security made simple.



SOPHOS

IPS Signature Update

Release Notes

Version : 9.16.40

Release Date : 30th October 2019

Release Information

Upgrade Applicable on

IPS Signature Release	Version 9.16.39
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 9.16.40 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 Four Hundred and Three(403) signatures to address Three Hundred and Forty One(341) vulnerabilities.

New signatures are added for the following vulnerabilities:

Name	CVE-ID	Category	Severity
BROWSER-CHROME Google Chrome Arbitrary Script Injection Vulnerability	CVE-2016- 5204	Browsers	1
BROWSER-CHROME Google Chrome CVE- 2013-6632 Denial Of Service	CVE-2016- 5200	Browsers	2
BROWSER-CHROME Google Chrome CVE- 2015-1233 Remote Code Execution	CVE-2016- 5200	Browsers	2
BROWSER-CHROME Google Chrome CVE- 2015-6764 Out of Bounds Memory Access	CVE-2016- 5200	Browsers	2
BROWSER-CHROME Google Chrome CVE- 2016-1653 Denial Of Service	CVE-2016- 1653	Browsers	2
BROWSER-CHROME Google Chrome CVE- 2016-1672 Same Origin Policy Bypass	CVE-2016- 1672	Browsers	2
BROWSER-CHROME Google Chrome CVE- 2016-1673 Universal Cross Site Scripting	CVE-2016- 6173	Browsers	2

BROWSER-CHROME Google Chrome CVE-2016-1675 Same Origin Policy	CVE-2016-1675	Browsers	2
BROWSER-CHROME Google Chrome CVE-2016-1676 Persistent Cross Site Scripting	CVE-2016-1676	Browsers	2
BROWSER-CHROME Google Chrome CVE-2016-1710 Same Origin Policy Bypass	CVE-2016-5129	Browsers	2
BROWSER-CHROME Google Chrome CVE-2016-5129 Denial Of Service	CVE-2016-5129	Browsers	2
BROWSER-CHROME Google Chrome CVE-2016-5200 Out of Bounds Memory Access	CVE-2016-5200	Browsers	2
BROWSER-CHROME Google Chrome CVE-2016-5207 Universal Cross Site Scripting	CVE-2016-5207	Browsers	2
BROWSER-CHROME Google Chrome CVE-2017-15396 Buffer Overflow	CVE-2016-5200	Browsers	2
BROWSER-CHROME Google Chrome CVE-2017-5007 Cross Site Scripting	CVE-2016-5129	Browsers	2
BROWSER-CHROME Google Chrome CVE-	CVE-2017-5040	Browsers	2

2017-5040 Out Of Bound Read			
BROWSER-CHROME Google Chrome CVE-2017-5088 Out of Bounds Memory Access	CVE-2017-5088	Browsers	2
BROWSER-CHROME Google Chrome CVE-2017-5122 Out Of Bound Memory Access	CVE-2017-5122	Browsers	2
BROWSER-CHROME Google Chrome CVE-2017-5129 Out Of Bound Memory Access	CVE-2017-5129	Browsers	2
BROWSER-CHROME Google Chrome CVE-2018-6056 Type Confusion	CVE-2016-5200	Browsers	2
BROWSER-CHROME Google Chrome Denial Of Service Vulnerability	CVE-2015-6771	Browsers	2
BROWSER-CHROME Google Chrome Denial Of Service Vulnerability	CVE-2016-1646	Browsers	2
BROWSER-CHROME Google Chrome Heap Corruption Vulnerability	CVE-2018-6064	Browsers	1
BROWSER-CHROME Google Chrome Heap Overflow Vulnerability	CVE-2017-5128	Browsers	1
BROWSER-CHROME Google Chrome Information Disclosure	CVE-2016-1665	Browsers	2

Vulnerability			
BROWSER-CHROME Google Chrome Information Disclosure Vulnerability	CVE-2016- 1677	Browsers	1
BROWSER-CHROME Google Chrome Information Disclosure Vulnerability	CVE-2016- 5172	Browsers	2
BROWSER-CHROME Google Chrome Object Corruption Vulnerability	CVE-2018- 6106	Browsers	1
BROWSER-CHROME Google Chrome Out Of Bounds Read Vulnerability	CVE-2017- 5098	Browsers	1
BROWSER-CHROME Google Chrome Out Of Bounds Vulnerability	CVE-2017- 5071	Browsers	1
BROWSER-CHROME Google Chrome Regexp Denial Of Service Vulnerability	CVE-2016- 1688	Browsers	2
BROWSER-CHROME Google Chrome Same Origin Policy Bypass Vulnerability	CVE-2015- 6770	Browsers	2
BROWSER-CHROME Google Chrome Same Origin Policy Bypass Vulnerability	CVE-2017- 0199	Browsers	1
BROWSER-CHROME Google Chrome Same	CVE-2017- 2480	Browsers	2

Origin Policy Bypass Vulnerability			
BROWSER-CHROME Google Chrome Same Remote Code Execution Vulnerability	CVE-2017-5008	Browsers	1
BROWSER-CHROME Google Chrome Use-After-Free Vulnerability	CVE-2017-5127	Browsers	1
BROWSER-CHROME Google Chrome V8 - Object Allocation Size Integer Overflow	CVE-2018-6065	Browsers	2
BROWSER-CHROME Google PDFium TIFF Image Flate Decoder Code Execution Vulnerability.	CVE-2015-7545	Browsers	1
BROWSER-FIREFOX Mozilla Firefox domFuzzLite3 table use after free attempt	CVE-2017-5404	Browsers	1
BROWSER-FIREFOX Mozilla Firefox method array.prototype.push remote code execution attempt	CVE-2018-12387	Browsers	2
BROWSER-IE Internet Explorer CVE-2017-8634 Remote Code Execution	CVE-2016-5129	Browsers	2
BROWSER-IE Internet Explorer Scripting Engine Memory	CVE-2017-11839	Browsers	1

Corruption Vulnerability			
BROWSER-IE Internet Explorer Scripting Engine Memory Corruption Vulnerability	CVE-2017-8645	Browsers	1
BROWSER-IE Internet Explorer Scripting Engine Memory Corruption Vulnerability	CVE-2017-8729	Browsers	1
BROWSER-IE Internet Explorer Scripting Engine Memory Corruption Vulnerability	CVE-2018-0840	Browsers	1
BROWSER-IE Microsoft Edge anonymous function type confusion attempt	CVE-2018-0774	Browsers	2
BROWSER-IE Microsoft Edge Chakra JIT BoundFunction NewInstance out of bounds read attempt	CVE-2018-8139	Browsers	2
BROWSER-IE Microsoft Edge Chakra JIT memory corruption attempt	CVE-2017-0234	Browsers	2
BROWSER-IE Microsoft Edge Chakra setPrototypeOf use-after-free attempt	CVE-2017-8751	Browsers	1
BROWSER-IE Microsoft Edge CVE-2017-11889 Scripting Engine postMessage Use After	CVE-2017-0236	Browsers	2

Free Attempt			
BROWSER-IE Microsoft Edge CVE-2017-8646 Remote Code Execution	CVE-2017-2363	Browsers	2
BROWSER-IE Microsoft Edge CVE-2017-8656 Remote Code Exec	CVE-2017-8656	Browsers	2
BROWSER-IE Microsoft Edge CVE-2018-0835 EnsureNonNativeArray Type Confusion I	CVE-2018-0835	Browsers	1
BROWSER-IE Microsoft Edge CVE-2019-0930 Information Disclosure	CVE-2019-0930	Browsers	2
BROWSER-IE Microsoft Edge out of bounds write attempt	CVE-2018-0777	Browsers	2
BROWSER-IE Microsoft Edge Scripting Engine CVE-2018-0770 Memory Corruption Vulnerability	CVE-2018-0770	Browsers	2
BROWSER-IE Microsoft Edge scripting engine memory corruption attempt	CVE-2018-0838	Browsers	1
BROWSER-IE Microsoft Edge scripting engine memory corruption attempt	CVE-2018-0980	Browsers	2
BROWSER-IE Microsoft Edge scripting engine memory corruption	CVE-2019-0991	Browsers	1

vulnerability attempt			
BROWSER-IE Microsoft Edge Scripting Engine Memory Corruption Vulnerability	CVE-2017-0134	Browsers	1
BROWSER-IE Microsoft Edge Scripting Engine Memory Corruption Vulnerability	CVE-2017-8740	Browsers	1
BROWSER-IE Microsoft Edge Scripting Engine Memory Corruption Vulnerability	CVE-2018-0837	Browsers	1
BROWSER-IE Microsoft Edge scripting engine type confusion attempt	CVE-2018-0775	Browsers	1
BROWSER-IE Microsoft Internet Explorer 11 CVE-2018-8619 VBScript Execution Policy Bypass	CVE-2018-8619	Browsers	1
BROWSER-IE Microsoft Internet Explorer CVE-2018-0763 Information Disclosure	CVE-2018-0763	Browsers	3
BROWSER-IE Microsoft Internet Explorer out of bounds read attempt	CVE-2017-11911	Browsers	1
BROWSER-IE Microsoft Internet Explorer out of bounds read attempt	CVE-2017-11911	Browsers	2
BROWSER-IE Microsoft Scripting Engine Memory Corruption	CVE-2017-0015	Browsers	1

Vulnerability			
BROWSER-IE Scripting Engine Memory Corruption Vulnerability Attempt	CVE-2017-11793	Browsers	1
BROWSER-OTHER Apple iTunes Denial Of Service Vulnerability	CVE-2018-4121	Browsers	1
BROWSER-OTHER Apple Safari CVE-2016-4734 Remote Code Execution	CVE-2016-4734	Browsers	2
BROWSER-OTHER Apple Safari CVE-2017-6980 Denial Of Service	CVE-2017-6980	Browsers	2
BROWSER-OTHER Apple Safari Remote Code Execution Vulnerability	CVE-2016-1857	Browsers	1
BROWSER-OTHER Apple Safari Remote Code Execution Vulnerability	CVE-2017-2491	Browsers	1
BROWSER-OTHER Apple Safari Same Origin Policy Bypass Vulnerability	CVE-2017-2365	Browsers	2
BROWSER-OTHER Safari Cross Site Scripting Vulnerability	CVE-2017-2504	Browsers	1
BROWSER-OTHER Safari Denial Of Service Vulnerability	CVE-2016-1779	Browsers	2
BROWSER-OTHER Safari Denial Of Service	CVE-2017-2531	Browsers	2

Vulnerability			
BROWSER-OTHER Safari Denial Of Service Vulnerability	CVE-2017-2547	Browsers	1
BROWSER-OTHER Safari Denial Of Service Vulnerability	CVE-2017-7056	Browsers	2
BROWSER-OTHER Safari Same Origin Policy Bypass Vulnerability	CVE-2017-2442	Browsers	2
BROWSER-OTHER Safari Same Origin Policy Bypass Vulnerability	CVE-2017-2446	Browsers	2
BROWSER-OTHER Safari Same Origin Policy Bypass Vulnerability	CVE-2017-2493	Browsers	2
BROWSER-OTHER Safari WebKit Remote Code Exceution Vulnerability	CVE-2017-2536	Browsers	1
BROWSER-WEBKIT Apple iOS WebKit Denial Of Service Vulnerability	CVE-2016-4622	Browsers	2
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-2017-2479 Universal Cross Site Scripting	CVE-2017-2479	Browsers	2
BROWSER-WEBKIT Apple Safari CVE-2017-2510 Universal Cross Site Scripting	CVE-2017-2510	Browsers	2
BROWSER-WEBKIT Apple Safari CVE-2017-2521 Denial Of service	CVE-2017-2521	Browsers	2
BROWSER-WEBKIT Apple Safari CVE-2017-2528 Universal Cross Site Scripting	CVE-2017-2528	Browsers	2
BROWSER-WEBKIT Apple Safari CVE-2017-7037 Denial Of Service	CVE-2017-7037	Browsers	2
BROWSER-WEBKIT Apple Safari CVE-2017-7089 Universal Cross Site Scripting	CVE-2017-7089	Browsers	2
BROWSER-WEBKIT Apple Safari CVE-2017-7117 Denial Of Service	CVE-2017-2363	Browsers	2
BROWSER-WEBKIT Apple Safari WebkitCVE-2017-2464 Denial Of Service	CVE-2017-2464	Browsers	2

BROWSER-WEBKIT Apple WebKit updateReferencedText use-after-free attempt	CVE-2018- 4315	Browsers	1
FILE-FLASH Adobe Flash Player CVE-2018-12826 Information Disclosure Vulnerability	CVE-2018- 12826	Multimedia	2
FILE-FLASH Adobe Flash Player Primetime SDK out of bounds read attempt	CVE-2016- 7873	Multimedia	1
FILE-IDENTIFY Adobe Acrobat JOBOPTIONS File Parsing Out of Bounds Read	CVE-2019- 7110	Application and Software	4
FILE-IDENTIFY Omron CX-Supervisor project file file attachment detected		Application and Software	4
FILE-IMAGE Adobe Acrobat EmfPlusDrawImagePoin ts out of bounds read attempt CVE-2018-5035	CVE-2018- 5035	Multimedia	2
FILE-IMAGE Adobe Acrobat Reader JPEG 2000 tile memory corruption attempt	CVE-2017- 11226	Multimedia	2
FILE-IMAGE Adobe Reader CVE-2018-5029 Out Of Bounds Read	CVE-2018- 5029	Multimedia	2
FILE-IMAGE Microsoft Windows OLE Load	CVE-2019- 0885	Multimedia	1

Picture remote code execution attempt			
FILE-MULTIMEDIA Adobe Acrobat Professional EMF malformed EMR_COMMENT record out of bounds access attempt	CVE-2017-11227	Multimedia	2
FILE-OFFICE Microsoft HTA Handler Vulnerability	CVE-2017-0199	Office Tools	1
FILE-OFFICE Microsoft Office directory traversal attempt	CVE-2019-0801	Office Tools	1
FILE-OFFICE Microsoft Office directory traversal attempt	CVE-2019-0801	Office Tools	2
FILE-OFFICE Microsoft Office Equation Editor RTF embedded OLE evasion attempt	CVE-2017-11882	Office Tools	2
FILE-OFFICE Microsoft Powerpoint graphics component remote code execution attempt	CVE-2019-0822	Office Tools	1
FILE-OTHER Acrobat Reader CVE-2018-12833 Information Disclosure Vulnerability	CVE-2018-12833	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-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 Use After Free Vulnerability	CVE-2019-7785	Application and Software	2
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	CVE-2019-7810	Application and Software	2

Out Of Bound Read Vulnerability			
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 docID Stack Buffer Overflow leak CVE-2018-4901	CVE-2018-4901	Application and Software	1
FILE-OTHER Adobe Acrobat and Reader docID Stack Buffer Overflow leak CVE-2018-4901	CVE-2018-4901	Application and Software	2
FILE-OTHER Adobe.Acrobat CVE-2018-16002 Out of Bounds Read	CVE-2018-16002	Application and Software	2
FILE-OTHER Adobe Acrobat CVE-2019-7040 use after free attempt	CVE-2019-7040	Application and Software	2
FILE-OTHER Adobe Acrobat EMF out-of-bounds read attempt	CVE-2018-16022	Application and Software	2

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-2019-7143	Application and Software	2
FILE-OTHER Adobe Acrobat PostScript parsing type confusion attempt	CVE-2019-7087	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 out of bounds read attempt	CVE-2018-15985	Application and Software	2
FILE-OTHER Adobe Acrobat Pro out of bounds read attempt	CVE-2018-16013	Application and Software	2
FILE-OTHER Adobe Acrobat Pro out of bounds read attempt	CVE-2018-16035	Application and Software	2
FILE-OTHER Adobe Acrobat Pro tiff parser out of bounds read attempt	CVE-2018-19705	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	CVE-2018-	Application	2

Acrobat Pro XPS file out-of-bounds read attempt	19714	and Software	
FILE-OTHER Adobe Acrobat Reader CVE-2019-7125 Arbitrary Code Execution	CVE-2019-7125	Application and Software	2
FILE-OTHER Adobe Photoshop CC & Bridge CC PNG File Parsing Vulnerability	CVE-2016-0951	Application and Software	1
FILE-OTHER Adobe Professional EMF embedded image heap overflow attempt CVE-2018-4982	CVE-2018-4982	Application and Software	1
FILE-OTHER Adobe Professional EMF polygon heap buffer overflow attempt	CVE-2017-11241	Application and Software	2
FILE-OTHER Adobe Reader CVE-2019-8019 Type Confusion	CVE-2019-8019	Application and Software	2
FILE-OTHER Adobe Reader EMF CVE-2018-16021 Heap Overflow	CVE-2018-16021	Application and Software	2
FILE-OTHER Apple iBook Information Disclosure Vulnerability	CVE-2017-2426	Application and Software	1
FILE-OTHER Cisco WebEx Recording Player memory corruption attempt	CVE-2018-0264	Application and Software	1

FILE-OTHER Microsoft SharePoint deserialization attempt	CVE-2019-1257	Application and Software	1
FILE-OTHER Microsoft Windows Avast Anti-Virus local credentials disclosure attempt	CVE-2018-12572	Application and Software	2
FILE-OTHER Microsoft Windows Device Guard bypass via compiled help file attempt	CVE-2017-8625	Application and Software	2
FILE-OTHER Microsoft Windows Jet Database CVE-2019-1249 Remote Code Execution	CVE-2019-7050	Application and Software	1
FILE-OTHER ReSIProcate CVE-2018-12584 preparseNewBytes Heap Buffer Overflow	CVE-	Application and Software	3
FILE-OTHER Snapd dirty_sock exploit download attempt	CVE-2019-7304	Application and Software	2
FILE-OTHER VideoLAN VLC media player out-of-bounds read attempt	CVE-2018-19857	Application and Software	1
FILE-OTHER VMware Fusion Guest VM Remote Code Execution	CVE-2019-5514	Application and Software	2
FILE-OTHER Windows GDI font out-of-bounds read attempt	CVE-2019-0758	Application and Software	1
FILE-PDF Adobe Acrobat and Reader Text Field	CVE-2019-7125	Application and Software	2

Value Remote Code Execution			
FILE-PDF Adobe Acrobat JavaScript engine out-of-bounds read attempt	CVE-2019-7053	Application and Software	1
FILE-PDF Adobe Acrobat JOBOPTIONS File Parsing Out of Bounds Read	CVE-2019-7110	Application and Software	1
FILE-PDF Adobe Acrobat PDF use-after-free attempt	CVE-2019-7050	Application and Software	2
FILE-PDF Adobe Acrobat Reader CVE-2019-7811 Out Of Bounds Read	CVE-2019-7811	Application and Software	2
FILE-PDF Adobe Acrobat Reader Forms Data Format embedded javascript attempt	CVE-2017-11229	Application and Software	2
FILE-PDF Adobe Acrobat Reader go-to action NTLM credential disclosure attempt	CVE-2018-4993	Application and Software	2
FILE-PDF Adobe Acrobat Reader JPEG2000 CVE-2016-6941 Information Disclosure Vulnerability	CVE-2016-6941	Application and Software	1
FILE-PDF Adobe Acrobat untrusted pointer dereference attempt	CVE-2017-16373	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-2018-5018 Out Of Bounds Read	CVE-2018-5018	Application and Software	2
FILE-PDF Adobe Reader CVE-2018-5031 Out Of Bounds Read	CVE-2018-5031	Application and Software	2
FILE-PDF Adobe Reader JavaScript resolveNode use-after-free attempt	CVE-2018-19708	Application and Software	2
FILE-PDF Adobe Reader JavaScript resolveNode use-after-free attempt	CVE-2018-19709	Application and Software	2
FILE-PDF Adobe Reader JavaScript resolveNode use-after-free Vulnerability	CVE-2018-19710	Application and Software	2
FILE-PDF Adobe Reader PDF CVE-2018-16047 Information Disclosure	CVE-2018-16047	Application and Software	2
FILE-PDF Microsoft Speech API remote code execution attempt	CVE-2019-0985	Application and Software	1
FILE-PDF TRUFFLEHUNTER TALOS-2018-0590 attack attempt	CVE-2018-12756	Application and Software	1
FILE-PDF TRUFFLEHUNTER TALOS-2018-0714 attack attempt	CVE-2019-7039	Application and Software	1

FILE-PDF TRUFFLEHUNTER TALOS-2019-0796 attack attempt		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-OTHER HWiNFO AMD64 Kernel Driver Information Disclosure	CVE-2018-6061	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 win32k driver buffer over read attempt	CVE-2019-1078	Operating System and Services	1
OS-WINDOWS Microsoft Windows COM Desktop Broker sandbox escape attempt	CVE-2019-0552	Operating System and Services	2
OS-WINDOWS Microsoft Windows Data Sharing Service privilege escalation attempt	CVE-2019-0573	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 Jet Database CVE-2019- 1243 Remote Code Execution	CVE-2019- 1243	Operating System and Services	2
OS-WINDOWS Microsoft Windows Jet Database CVE-2019- 1243 Remote Code Execution	CVE-2019- 1243	Operating System and Services	4
OS-WINDOWS Microsoft Windows SMB Transaction heap groom attempt		Operating System and Services	3
OS-WINDOWS Microsoft Windows win32k NtGdiExtFloodFill memory corruption attempt	CVE-2019- 1017	Operating System and Services	1
OS-WINDOWS Windows OLE Automation Array Remote Code Execution Vulnerability	CVE-2014- 6332	Operating System and Services	1
PROTOCOL-SCADA Advantech CVE-2019- 3953 WebAccess SCADA IOCTL 10012 Stack Buffer Overflow	CVE-2019- 3953	FTP	2
PROTOCOL-SCADA	CVE-2019-	FTP	2

Advantech WebAccess SCADA viewdll1 Stack Buffer Overflow	3954		
PUA-OTHER CoinHive Miner client detected		Malware Communication	2
SERVER-APACHE Apache ActiveMQ CVE-2018-8006 Web Console QueueFilter Cross-Site Scripting	CVE-2018-8006	Apache HTTP Server	1
SERVER-APACHE Apache Qpid Sequence Set Denial of Service	CVE-2015-0203	Apache HTTP Server	1
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 Struts java.lang.ProcessBuilder class access attempt	CVE-2018-11776	Apache HTTP Server	2
SERVER-APACHE Apache Struts ognl remote code execution attempt	CVE-2018-11776	Apache HTTP Server	2
SERVER-OTHER Adobe ColdFusion arbitrary file upload attempt CVE-2019-7816	CVE-2019-7816	Application and Software	2
SERVER-OTHER Adobe ColdFusion CKEditor upload.cfm Unrestricted File Upload CVE-2018-	CVE-2018-15961	Other Web Server	2

15961			
SERVER-OTHER Advantech WebAccess Node spchapi and tv_enua Stack Buffer Overflow		Other Web Server	2
SERVER-OTHER ASP webshell upload attempt		Other Web Server	4
SERVER-OTHER Century Star SCADA directory traversal attempt		Other Web Server	2
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 CFM webshell upload attempt		Other Web Server	4
SERVER-OTHER Cisco ASA VPN aggregateAuthDataHan dler double free attempt	CVE-2018- 0101	Other Web Server	1
SERVER-OTHER Cisco IOS XE REST API Authentication Bypass	CVE-2019- 12643	Other Web Server	2
SERVER-OTHER Cisco Prime Infrastructure and EPNM UploadServlet Tar	CVE-2019- 1821	Other Web Server	2

Directory Traversal			
SERVER-OTHER Cisco Prime Infrastructure swimtemp CVE-2018-15379 TFTP Arbitrary File Upload		Other Web Server	2
SERVER-OTHER Cisco Software Cluster Management Protocol remote code execution attempt	CVE-2017-3881	Other Web Server	1
SERVER-OTHER EMC Data Protection CVE-2017-8013 Advisor Application Service Static Credentials Authentication Bypass	CVE-2017-8013	Other Web Server	3
SERVER-OTHER Flexense Syncbreeze buffer overflow attempt	CVE-2018-5262	Other Web Server	1
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 dbman FileTrans Arbitrary File Write	CVE-2017-5822	Other Web Server	1
SERVER-OTHER HPE Intelligent Management Center dbman Stack Buffer Overflow	CVE-2018-7115	Other Web Server	2

SERVER-OTHER HPE Intelligent Management Center TopoDebugServlet Insecure Deserialization		Other Web Server	2
SERVER-OTHER IBM WebSphere Application Server Commons- Collections Library Remote Code Execution	CVE-2015- 7450	Other Web Server	1
SERVER-OTHER Interactive Graphical SCADA System arbitrary file read attempt		Other Web Server	1
SERVER-OTHER ipTime G104BE directory traversal attempt		Other Web Server	2
SERVER-OTHER Jenkins CI Server Groovy Pipeline Remote Code Execution	CVE-2019- 1003001	Other Web Server	1
SERVER-OTHER libVNC LibVNCClient CoRRE Heap-based Buffer Overflow CVE-2018- 20020	CVE-2018- 20020	Other Web Server	2
SERVER-OTHER libVNC LibVNCServer File Transfer Extension Heap-based Buffer Overflow	CVE-2018- 15127	Other Web Server	2
SERVER-OTHER Microsoft JET Database Engine CVE-2018-8423 Remote Code Execution	CVE-2018- 8423	Other Web Server	2

Vulnerability			
SERVER-OTHER Netatalk dsi_opensession Attention Quantum Out-of-bounds Write	CVE-2018- 1160	Other Web Server	1
SERVER-OTHER Network Time Protocol ntpq decodearr Stack-based Buffer Overflow CVE- 2018-7183	CVE-2018- 7183	Other Web Server	2
SERVER-OTHER NFS server /etc/passwd symlink creation attempt	CVE-2019- 11538	Other Web Server	3
SERVER-OTHER NFS server /etc/passwd symlink creation attempt		Other Web Server	3
SERVER-OTHER Nginx Unit Router Process Heap-based Buffer Overflow	CVE-2019- 7401	Other Web Server	2
SERVER-OTHER ntpq decode array buffer overflow attempt CVE- 2018-7183	CVE-2018- 7183	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 Out of Bounds Read	CVE-2019- 6444	Other Web Server	1

SERVER-OTHER NUUO NVRMini2 stack based buffer overflow attempt	CVE-2018-1149	Other Web Server	2
SERVER-OTHER Perl webshell upload attempt		Other Web Server	2
SERVER-OTHER PHP webshell upload attempt		Other Web Server	4
SERVER-OTHER Pivotal Spring Framework CVE-2018-1273 isWritableProperty SpEL Injection	CVE-2018-1273	Other Web Server	2
SERVER-OTHER Rockwell Automation RSLinx Classic Forward Open Electronic Key Stack Buffer Overflow	CVE-2019-6553	Other Web Server	2
SERVER-OTHER Samsung Integrated Management System Data Management Server hardcoded credentials attempt		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 Zoho ManageEngine OpManager APIDBUtl getDevicesForSearchStri	CVE-2018-17243	Other Web Server	2

ng SQL Injection			
SERVER-WEBAPP Adobe ColdFusion CVE-2018-15959 DataServicesCFProxy Commons BeanUtils Insecure Deserialization	CVE-2018-15959	Web Services and Applications	3
SERVER-WEBAPP Alcatel Lucent I-240W-Q GPON ONT Stack Buffer Overflow Vulnerability	CVE-2019-3921	Web Services and Applications	1
SERVER-WEBAPP All in One Video Downloader SQL injection attempt		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 Superset python pickle library remote code execution attempt	CVE-2018-8021	Apache HTTP Server	1
SERVER-WEBAPP Atlassian confluence widget remote code execution attempt	CVE-2019-3396	Web Services and Applications	1
SERVER-WEBAPP Bacula-Web client-report.php SQL injection attempt	CVE-2017-15367	Web Services and Applications	2
SERVER-WEBAPP Bacula-Web jobs.php	CVE-2017-	Web Services and	2

SQL injection attempt	15367	Applications	
SERVER-WEBAPP CentOS Web Panel persistent cross site scripting attempt	CVE-2019- 7646	Web Services and Applications	2
SERVER-WEBAPP Cisco IOS XE WebUI Command Injection Vulnerability	CVE-2019- 12651	Web Services and Applications	2
SERVER-WEBAPP CloudByte ElastiStor imageUploadServlet directory traversal attempt	CVE-2018- 15675	Web Services and Applications	2
SERVER-WEBAPP CMS Made Simple arbitrary PHP file upload attempt	CVE-2018- 1000094	Web Services and Applications	4
SERVER-WEBAPP CMS Made Simple server side template injection attempt	CVE-2017- 16783	Web Services and Applications	2
SERVER-WEBAPP CMSsite 1.0 SQL injection attempt		Web Services and Applications	2
SERVER-WEBAPP Cobub Razor channel name SQL injection attempt	CVE-2018- 8057	Web Services and Applications	2
SERVER-WEBAPP Cogent DataHub SQL injection attempt		Web Services and Applications	2
SERVER-WEBAPP CyberArk Enterprise Password Vault XML	CVE-2019- 7442	Web Services and Applications	2

external entity injection attempt			
SERVER-WEBAPP DoD IT Solutions Homey BnB script SQL injection attempt		Web Services and Applications	2
SERVER-WEBAPP Easy Hosting Control Panel action cross site scripting attempt	CVE-2018-6362	Web Services and Applications	2
SERVER-WEBAPP Epic MyChart SQL injection attempt	CVE-2016-6272	Web Services and Applications	2
SERVER-WEBAPP EventManager page.php sql injection attempt SQL injection attempt	CVE-2018-6576	Web Services and Applications	1
SERVER-WEBAPP Flexpaper and Flowpaper command injection attempt	CVE-2018-11686	Web Services and Applications	2
SERVER-WEBAPP Fortigate SSL VPN cross site scripting attempt	CVE-2018-13380	Web Services and Applications	2
SERVER-WEBAPP generic cross site scripting via url attempt		Web Services and Applications	2
SERVER-WEBAPP Git Remote Code Execution Vulnerability	CVE-2015-7545	Web Services and Applications	1
SERVER-WEBAPP Gxlcms SQL injection	CVE-2018-9247	Web Services and	2

attempt		Applications	
SERVER-WEBAPP HAProxy H2 Frame heap memory corruption attempt	CVE-2018- 10184	Web Services and Applications	1
SERVER-WEBAPP Horde Groupware Webmail Contact Management add.php directory traversal attempt		Web Services and Applications	2
SERVER-WEBAPP Horde Groupware Webmail encryptMessage prefs.php command injection attempt	CVE-2017- 7413	Web Services and Applications	2
SERVER-WEBAPP HPE IMC CustomReportTemplate SelectBean Expression Language Injection	CVE-2019- 5373	Web Services and Applications	1
SERVER-WEBAPP HPE Intelligent Management Center ByteMessageResource Insecure Deserialization	CVE-2019- 11956	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 Network Automation PermissionFilter Authentication Bypass (Decrypted Traffic)	CVE-2017- 5812	Web Services and Applications	3

SERVER-WEBAPP HPE Network CVE-2017- 5812 Automation PermissionFilter Authentication Bypass	CVE-2017- 5812	Web Services and Applications	3
SERVER-WEBAPP IBM WebSphere Application Server remote code execution attempt	CVE-2019- 4279	Web Services and Applications	2
SERVER-WEBAPP IceWarp Mail Server directory traversal attempt	CVE-2015- 1503	Web Services and Applications	2
SERVER-WEBAPP Intenos lopsys Remote Code Execution Vulnerability	CVE-2017- 17867	Web Services and Applications	1
SERVER-WEBAPP Jenkins Groovy metaprogramming remote code execution attempt	CVE-2019- 1003000	Web Services and Applications	2
SERVER-WEBAPP Joomla ProjectLog search SQL injection attempt	CVE-2018- 6024	Web Services and Applications	2
SERVER-WEBAPP LG- Ericsson iPECS NMS 30M directory traversal attempt	CVE-2018- 15138	Web Services and Applications	2
SERVER-WEBAPP MailCleaner managetracing searchAction command injection attempt		Web Services and Applications	2

SERVER-WEBAPP ManageEngine Applications Manager MenuHandlerServlet SQL Injection	CVE-2016- 9488	Web Services and Applications	1
SERVER-WEBAPP ManageEngine Applications Manager showActionProfiles.do SQL injection attempt	CVE-2017- 16850	Web Services and Applications	2
SERVER-WEBAPP ManageEngine Applications Manager testCredential.do command injection attempt	CVE-2018- 7890	Web Services and Applications	1
SERVER-WEBAPP Manage Engine Recovery Manager cross site scripting attempt	CVE-2018- 9163	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 EntityInstanceIdEncoder remote code execution attempt	CVE-2019- 0604	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 Multiple products HTML5 ping DDoS attempt		Web Services and Applications	3
SERVER-WEBAPP Network Time Protocol ntpq decodearr Stack- based Buffer Overflow	CVE-2018- 7183	Web Services and Applications	1
SERVER-WEBAPP NUUO NVRmini upgrade_handle.php command injection attempt	CVE-2018- 14933	Web Services and Applications	2
SERVER-WEBAPP OpenEMR ajax_download.php Directory Traversal	CVE-2019- 14530	Web Services and Applications	2
SERVER-WEBAPP OpenEMR C_Document.class.php patient_id Cross-Site Scripting	CVE-2019- 3963	Web Services and Applications	2
SERVER-WEBAPP OpenEMR SQL injection attempt	CVE-2018- 9250	Web Services and Applications	2
SERVER-WEBAPP Oracle Business Intelligence directory traversal attempt	CVE-2019- 2588	Web Services and Applications	2
SERVER-WEBAPP Orchid Core VMS Unauthenticated Priviledged Directory Traversal	CVE-2018- 10956	Web Services and Applications	2

SERVER-WEBAPP OWASP ModSecurity Core Rule Set CVE-2018- 16384 Sql Injection	CVE-2018- 16384	Web Services and Applications	2
SERVER-WEBAPP PHP CVE-2018-5711 Denial Of Service	CVE-2018- 5711	Web Services and Applications	2
SERVER-WEBAPP ProjectSend SQL injection Vulnerability	CVE-2018- 13452	Web Services and Applications	2
SERVER-WEBAPP Pulse Secure diag.cgi Command Injection (Decrypted Traffic)	CVE-2019- 11539	Web Services and Applications	1
SERVER-WEBAPP Pulse Secure diag.cgi Command Injection (encrypted Traffic)	CVE-2019- 11539	Web Services and Applications	1
SERVER-WEBAPP Pulse Secure diag.cgi Command Injection	CVE-2019- 11539	Web Services and Applications	2
SERVER-WEBAPP Pulse Secure Guacamole URI Information Disclosure (Decrypted Traffic)	CVE-2019- 11510	Web Services and Applications	2
SERVER-WEBAPP Pulse Secure Guacamole URI Information Disclosure (encrypted Traffic)	CVE-2019- 11510	Web Services and Applications	2
SERVER-WEBAPP Pulse Secure Platform Stack- Based Buffer Overflow (Decrypted Traffic)	CVE-2019- 11542	Web Services and Applications	1

SERVER-WEBAPP Pulse Secure Platform Stack-Based Buffer Overflow (encrypted Traffic)	CVE-2019-11542	Web Services and Applications	1
SERVER-WEBAPP QNAP QCenter API date_config command injection attempt	CVE-2018-0709	Web Services and Applications	2
SERVER-WEBAPP Quest DR Series Disk Backup CustomerPortalService.pm command injection attempt	CVE-2018-11181	Web Services and Applications	2
SERVER-WEBAPP Quest DR Series Disk Backup EncryptionService.pm command injection attempt	CVE-2018-11176	Web Services and Applications	2
SERVER-WEBAPP Ruby Net FTP library command injection attempt	CVE-2017-17405	Web Services and Applications	2
SERVER-WEBAPP Ruby on Rails Action View Information Disclosure	CVE-2019-5418	Web Services and Applications	2
SERVER-WEBAPP Ruby on Rails Active Storage deserialization remote code execution attempt	CVE-2019-5420	Web Services and Applications	1
SERVER-WEBAPP Samsung Web Viewer Cross Site Scripting Vulnerability	CVE-2018-11689	Web Services and Applications	2
SERVER-WEBAPP	CVE-2016-	Web Services	2

Seowonintech diagnostic.cgi command injection attempt	10760	and Applications	
SERVER-WEBAPP Seowonintech system_config.cgi local file include attempt	CVE-2016- 10760	Web Services and Applications	2
SERVER-WEBAPP Sitefinity WCMS cross site scripting attempt	CVE-2018- 17053	Web Services and Applications	2
SERVER-WEBAPP Sitefinity WCMS cross- site scripting attempt	CVE-2018- 17056	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 Softneta MedDream PACS Server Premium directory traversal attempt		Web Services and Applications	2
SERVER-WEBAPP SolusLabs SolusVM centralbackup.php SQL injection attempt		Web Services and Applications	2
SERVER-WEBAPP Subsonic Subscribe to Podcast cross site scripting attempt	CVE-2017- 9414	Web Services and Applications	2
SERVER-WEBAPP Telerik UI cryptographic keys disclosure attempt	CVE-2017- 9248	Web Services and Applications	2

SERVER-WEBAPP ThinkPHP 5.0.23/5.1.31 command injection attempt		Web Services and Applications	2
SERVER-WEBAPP ThinkPHP command injection attempt		Web Services and Applications	2
SERVER-WEBAPP ThinkPHP SQL injection attempt		Web Services and Applications	2
SERVER-WEBAPP TPLink TD W8151N SQL injection attempt		Web Services and Applications	2
SERVER-WEBAPP Tpshop remote file include attempt	CVE-2018- 9919	Web Services and Applications	2
SERVER-WEBAPP Trend Micro Control Manager SQL injection attempt	CVE-2018- 3606	Web Services and Applications	2
SERVER-WEBAPP Trend Micro DDEI directory traversal attempt		Web Services and Applications	2
SERVER-WEBAPP Unitrends Enterprise Backup Appliance download-files command injection attempt	CVE-2017- 7283	Web Services and Applications	2
SERVER-WEBAPP vBulletin SQL injection attempt	CVE-2019- 17271	Web Services and Applications	2
SERVER-WEBAPP VMWare NSX SD-WAN	CVE-2018- 6961	Web Services and	1

Edge command injection attempt		Applications	
SERVER-WEBAPP Webadmin history parameter cross site scripting attempt	CVE-2018-19191	Web Services and Applications	2
SERVER-WEBAPP Webadmin history parameter cross site scripting attempt	CVE-2018-9250	Web Services and Applications	2
SERVER-WEBAPP WIFICAM Wireless IP Camera command injection attempt	CVE-2017-18377	Web Services and Applications	2
SERVER-WEBAPP WordPress default admin theme cross site scripting attempt		Web Services and Applications	2
SERVER-WEBAPP WordPress Rencontre plugin SQL injection attempt	CVE-2019-13413	Web Services and Applications	2
SERVER-WEBAPP WordPress Yuzo Related Posts plugin cross site scripting attempt		Web Services and Applications	2
SERVER-WEBAPP Zoho ManageEngine OpManager APIDBUtl getDevicesForSearchString SQL Injection	CVE-2018-17243	Web Services and Applications	2

- **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

©1997 - 2019 Sophos Ltd. All rights reserved.

All rights reserved. Sophos, Sophos logo are trademark of Sophos Technologies Pvt. Ltd.

Corporate Headquarters

Sophos Technologies Pvt. Ltd.

Reg. Office: Sophos House, Saigulshan Complex,

Beside White House, Panchvati Cross Road,

Ahmedabad – 380006, INDIA

Phone: +91-79-66216666

Fax: +91-79-26407640

Web site: www.sophos.com