SOPHOS
Security made simple.

SOPHOS
IPS Signature Update
Release Notes

Version : 7.16.68
Release Date : 21st January 2020

Release Information

Upgrade Applicable on

IPS Signature Release	Version 7.16.67
Sophos Appliance Models	XG-550, XG-750, XG-650

Upgrade Information

Upgrade type: Automatic

Compatibility Annotations: None

Introduction

The Release Note document for IPS Signature Database Version 7.16.68 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 Seventy One(471) signatures to address Three Hundred and Eighty Five(385) vulnerabilities.

New signatures are added for the following vulnerabilities:

Name	CVE–ID	Category	Severity
BROWSER-CHROME Google Chrome CVE-2015-1256 blink buildShadowAndInstanceTree Use After Free II	CVE-2015-1256	Browsers	2
BROWSER-CHROME Google Chrome CVE-2015-1256 blink buildShadowAndInstanceTree Use After Free I	CVE-2015-1256	Browsers	2
BROWSER-CHROME Google Chrome CVE-2017-5112 WebGL 2 ReadPixels Heap Buffer Overflow II	CVE-2017-5112	Browsers	1
BROWSER-FIREFOX Mozilla Firefox CVE-2013-1690 onreadystatechange Use After Free	CVE-2013-1690	Browsers	1
BROWSER-FIREFOX Mozilla Firefox http-index-format CVE-2017-5444 File Out-Of-Bounds Read	CVE-2017-5444	Browsers	2
BROWSER-IE Microsoft CVE-2004-0719 Internet Explorer Frame Injection Vulnerability	CVE-2004-0719	Browsers	1

BROWSER-IE Microsoft CVE-2012-0171 Internet Explorer SelectAll Use-after-free	CVE-2012-0171	Browsers	1
BROWSER-IE Microsoft Edge CVE-2016-0193 Array.prototype.fill Out of Bounds Write Attempt	CVE-2016-0193	Browsers	2
BROWSER-IE Microsoft Edge CVE-2016-3271 ArrayBuffer.transfer Information Disclosure Attempt	CVE-2016-3271	Browsers	3
BROWSER-IE Microsoft Edge CVE-2016-3370 PDF out-of-bounds Crypt Filter length attempt	CVE-2016-3370	Browsers	1
BROWSER-IE Microsoft Edge CVE-2016-3370 PDF out-of-bounds Crypt Filter Length	CVE-2016-3370	Browsers	1
BROWSER-IE Microsoft Edge CVE-2016-3386 Spread Operator Memory Corruption Attempt	CVE-2016-3386	Browsers	2
BROWSER-IE Microsoft Edge CVE-2017-11764 Chakra ParseCatch Type Confusion I	CVE-2017-11764	Browsers	2
BROWSER-IE Microsoft Edge CVE-2017-11811 DoLoopBodyStart Out	CVE-2017-11811	Browsers	2

of Bounds Read II			
BROWSER-IE Microsoft Edge CVE-2017-11811 DoLoopBodyStart Out of Bounds Read I	CVE-2017-11811	Browsers	2
BROWSER-IE Microsoft Edge CVE-2017-8603 AsmJsInterpreter Use After Free II	CVE-2017-8603	Browsers	1
BROWSER-IE Microsoft Edge CVE-2017-8603 AsmJsInterpreter Use After Free I	CVE-2017-8603	Browsers	1
BROWSER-IE Microsoft Edge CVE-2017-8652 Use After Free	CVE-2017-8652	Browsers	1
BROWSER-IE Microsoft Edge CVE-2018-0858 Scripting Engine Memory Corruption Attempt	CVE-2018-0858	Browsers	2
BROWSER-IE Microsoft Edge PDF out-of-bounds Crypt Filter Length Attempt III	CVE-2016-3370	Browsers	2
BROWSER-IE Microsoft Edge PDF Reader CVE-2016-3203 Out Of Bounds Memory Access Attempt	CVE-2016-3203	Browsers	2
BROWSER-IE Microsoft Edge Scripting Engine memory corruption attempt	CVE-2018-0834	Browsers	2

BROWSER-IE Microsoft Edge scripting engine type confusion attempt	CVE-2018-0860	Browsers	2
BROWSER-IE Microsoft Internet Explorer MutationObserver use after free attempt	CVE-2015-2425	Browsers	2
BROWSER-IE Microsoft Internet Explorer 5 Compatibility Mode Use After Free Attempt	CVE-2013-3121	Browsers	2
BROWSER-IE Microsoft Internet Explorer 8 CSS Invalid Mapping Exploit Attempt	CVE-2010-3328	Browsers	1
BROWSER-IE Microsoft Internet Explorer 9 CTreeNode Use After Free Attempt	CVE-2012-1878	Browsers	2
BROWSER-IE Microsoft Internet Explorer 9 onbeforeprint Use After Free Attempt	CVE-2013-0092	Browsers	1
BROWSER-IE Microsoft Internet Explorer 9 MutationEvent Use After Free Attempt	CVE-2013-3207	Browsers	1
BROWSER-IE Microsoft Internet Explorer Clone Object Reference	CVE-2007-3903	Browsers	3

Memory Corruption			
BROWSER-IE Microsoft Internet Explorer COM Object Instantiation Memory Corruption (1)	CVE-2005-1990	Browsers	3
BROWSER-IE Microsoft Internet Explorer CTableCell get_cellIndex Information Disclosure II		Browsers	3
BROWSER-IE Microsoft Internet Explorer cve-2006-2382 HTML Decoding Memory Corruption Attempt	CVE-2006-2382	Browsers	1
BROWSER-IE Microsoft Internet Explorer CVE-2010-3345 Select Element Memory Corruption	CVE-2010-3345	Browsers	2
BROWSER-IE Microsoft Internet Explorer CVE-20111-1993 onscroll DOS Attempt	CVE-2011-1993	Browsers	2
BROWSER-IE Microsoft Internet Explorer CVE-2012-0171 SelectAll Dangling Pointer Use After Free Attempt	CVE-2012-0171	Browsers	1
BROWSER-IE Microsoft Internet Explorer CVE-2012-1876 html table column span width increase memory corruption attempt	CVE-2012-1876	Browsers	2

BROWSER-IE Microsoft Internet Explorer CVE-2012-4792 applyElement Use After Free (Published Exploit)	CVE-2012-4792	Browsers	2
BROWSER-IE Microsoft Internet Explorer CVE-2012-4792 applyElement Use After Free	CVE-2012-4792	Browsers	2
BROWSER-IE Microsoft Internet Explorer CVE-2013-1347 CGenericElement Memory Corruption I	CVE-2013-1347	Browsers	1
BROWSER-IE Microsoft Internet Explorer CVE-2013-2551 VML Array With Negative Length Memory Corruption Attempt	CVE-2013-2551	Browsers	1
BROWSER-IE Microsoft Internet Explorer CVE-2013-3163 Use After Free Attempt	CVE-2013-3163	Browsers	2
BROWSER-IE Microsoft Internet Explorer CVE-2013-3163 Use After Free	CVE-2013-3163	Browsers	2
BROWSER-IE Microsoft Internet Explorer CVE-2014-0305 pastHTML Use After Free I	CVE-2014-0305	Browsers	1
BROWSER-IE Microsoft Internet Explorer CVE-	CVE-2015-0041	Browsers	2

2015-0041 CTreeDataPos Use-After-Free Remote Code Execution Attempt			
BROWSER-IE Microsoft Internet Explorer CVE-2016-0061 CallInvoke Type Confusion Attempt	CVE-2016-0061	Browsers	2
BROWSER-IE Microsoft Internet Explorer CVE-2016-0106 SetItem Use After Free Attempt II	CVE-2016-0106	Browsers	1
BROWSER-IE Microsoft Internet Explorer CVE-2016-0169 EMF file integer overflow attempt	CVE-2016-0169	Browsers	2
BROWSER-IE Microsoft Internet Explorer CVE-2016-0186 Uninitialized Pointer Attempt I	CVE-2016-0186	Browsers	1
BROWSER-IE Microsoft Internet Explorer InitFromString Function Out of Bounds Memory Access II	CVE-2015-6086	Browsers	3
BROWSER-IE Microsoft Internet Explorer JPEG Rendering Buffer Overflow	CVE-2005-1988	Browsers	2
BROWSER-IE Microsoft Internet Explorer Location Property Cross Domain Scripting	CVE-2008-2947	Browsers	3

BROWSER-IE Microsoft Internet Explorer Mouse Movement Information Disclosure II		Browsers	1
BROWSER-IE Microsoft Internet Explorer toStaticHTML Cross Site Scripting	CVE-2010-1257	Browsers	3
BROWSER-OTHER Opera Browser Content Length Buffer Overflow II		Browsers	1
BROWSER-OTHER Opera Browser Content Length Buffer Overflow I		Browsers	1
BROWSER-OTHER Opera Software Opera GIF Processing Memory Corruption III		Browsers	1
BROWSER-OTHER Opera Software Opera GIF Processing Memory Corruption I		Browsers	1
BROWSER-OTHER test_html		Browsers	1
BROWSER-OTHER test_uri		Browsers	1
BROWSER-PLUGINS Adobe Acrobat Reader AdobePDF ActiveX Use After Free	CVE-2014-0527	Browsers	1

BROWSER-PLUGINS Advantech WebAccess CVE-2014-9208 AspVCObj.AspDataDriven GetWideStrCpy ActiveX Clsid Access II	CVE-2014-9208	Browsers	1
BROWSER-PLUGINS Advantech WebAccess CVE-2014-9208 AspVCObj.AspDataDriven GetWideStrCpy ActiveX Stack Overflow II	CVE-2014-9208	Browsers	2
BROWSER-PLUGINS Advantech WebAccess SCADA CVE-2014-0991 ProjectName Parameter Buffer Overflow II	CVE-2014-0991	Browsers	2
BROWSER-PLUGINS Advantech WebAccess SCADA CVE-2014-0991 ProjectName Parameter Buffer Overflow I	CVE-2014-0991	Industrial Control System	2
BROWSER-PLUGINS Cisco Webex Meeting Manager atucfobj ActiveX Control Buffer Overflow II	CVE-2008-3558	Browsers	2
BROWSER-PLUGINS HP PoS CVE-2014-7890 OPOS Driver opostoneindicator.ocx Open Method Stack Overflow	CVE-2014-7890	Browsers	2
BROWSER-PLUGINS IBM Access Support ActiveX GetXMLValue Method	CVE-2009-0215	Browsers	1

Buffer Overflow			
BROWSER-PLUGINS IBM SPSS CVE-2012-0189 VsVIEW6.ocx ActiveX Control Code Execution II	CVE-2012-0189	Browsers	1
BROWSER-PLUGINS IBM SPSS CVE-2012-0189 VsVIEW6.ocx ActiveX Control Code Execution I	CVE-2012-0189	Browsers	1
BROWSER-PLUGINS IBM SPSS SamplePower CVE-2012-5945 Vsflex8l ActiveX Control Buffer Overflow	CVE-2012-5945	Browsers	2
BROWSER-PLUGINS McAfee ePolicy Orchestrator SiteManager CVE-2007-1498 ActiveX Control ExportSiteList Buffer Overflow	CVE-2007-1498	Browsers	1
BROWSER-PLUGINS Microsoft Silverlight CVE-2013-3178 Null Pointer Dereference Code Execution	CVE-2013-3178	Browsers	2
BROWSER-PLUGINS Microsoft Silverlight CVE-2013-3896 WriteableBitmap SetSource Information Disclosure	CVE-2013-3896	Browsers	3
BROWSER-PLUGINS Microsoft Windows	CVE-2013-	Browsers	1

CVE-2013-1296 Remote Desktop Client ActiveX Control Use After Free	1296		
BROWSER-PLUGINS Microsoft Windows CVE-2013-1296 Remote Desktop Client ActiveX Control Use After Free	CVE-2013-1296	Browsers	2
BROWSER-PLUGINS Microsoft WMI Administrative Tools ActiveX Control Multiple Vulnerabilities II	CVE-2010-3973	Browsers	2
BROWSER-PLUGINS Novell iPrint Client Remote File Deletion		Browsers	1
BROWSER-PLUGINS Oracle Document Capture EasyMail IMAP4 LicenseKey Buffer Overflow		Browsers	3
BROWSER-PLUGINS Samsung iPOLiS Device Manager CVE-2015-0555 WriteConfigValue Stack Buffer Overflow Vulnerability	CVE-2015-0555	Browsers	1
BROWSER-PLUGINS Schneider Electric CVE-2014-9200 Multiple Products IsObjectModel RemoveParameter Stack Buffer Overflow	CVE-2014-9200	Browsers	2
BROWSER-PLUGINS Schneider Electric CVE-2015-0982 Pelco DS-	CVE-2015-0982	Browsers	3

NVs Rvctl.RVControl.1 Buffer Overflow			
BROWSER-PLUGINS Siemens SIMATIC CVE-2013-0674 WinCC RegReader ActiveX Vulnerable Function Access Attempt	CVE-2013-0674	Browsers	3
BROWSER-PLUGINS WebGate CVE-2015-2094 Multiple Products WESPPlaybackCtrl Two Stack Buffer Overflow	CVE-2015-2094	Browsers	3
BROWSER-PLUGINS Yahoo! Widgets YDP ActiveX Control Buffer Overflow	CVE-2007-4034	Browsers	1
BROWSER-WEBKIT Apple Safari Webkit CVE-2011-1774 libxslt Arbitrary File Creation	CVE-2011-1774	Browsers	2
FILE-EXECUTABLE Microsoft Windows .NET Framework CVE-2012-1855 xbap DataObject Object Pointer Attempt	CVE-2012-1855	Application and Software	2
FILE-FLASH Adobe Flash CVE-2014-0556 copyPixelsToByteArray integer overflow attempt	CVE-2014-0556	Multimedia	2
FILE-FLASH Adobe Flash Player CVE-2011-0611 ActionScript callMethod Type Confusion Code	CVE-2011-0611	Multimedia	1

Execution III			
FILE-FLASH Adobe Flash Player CVE-2011-0611 ActionScript callMethod Type Confusion Code Execution II	CVE-2011-0611	Multimedia	1
FILE-FLASH Adobe Flash Player CVE-2011-0611 ActionScript callMethod Type Confusion Code Execution I	CVE-2011-0611	Multimedia	1
FILE-FLASH Adobe Flash Player CVE-2018-2848 Use After Free II	CVE-2018-4878	Multimedia	1
FILE-FLASH Adobe Flash Player CVE-2018-2848 Use After Free I	CVE-2018-4878	Multimedia	1
FILE-FLASH Adobe Flash Player Invalid Object Reference Code Execution (Published Exploit)	CVE-2009-0520	Multimedia	2
FILE-FLASH Adobe Flash Player malformed ATF buffer overflow attempt	CVE-2018-4871	Multimedia	2
FILE-IMAGE Adobe Acrobat Pro CVE-2017-16381 SampleFormat heap overflow attempt	CVE-2017-16381	Multimedia	2
FILE-IMAGE Adobe Photoshop CS4 ABR File Processing Buffer Overflow	CVE-2010-1296	Multimedia	2

FILE-IMAGE Apple QuickTime CVE-2008-1019 PICT Multiple Records Handling Buffer Overflow	CVE-2008-1019	Multimedia	2
FILE-IMAGE ImageMagick CVE-2013-4298 GIF Comment Processing Off-by-one Buffer Overflow II	CVE-2013-4298	Multimedia	2
FILE-IMAGE ImageMagick CVE-2013-4298 GIF Comment Processing Off-by-one Buffer Overflow I	CVE-2013-4298	Multimedia	2
FILE-IMAGE ImageMagick SyncExifProfile Out Of Bounds Array Indexing	CVE-2016-7799	Multimedia	3
FILE-JAVA Oracle Java CVE-2011-0802 FileDialog.Show Heap Buffer Overflow	CVE-2011-0802	Application and Software	2
FILE-JAVA Oracle Java Font Parsing maxPoints Heap Buffer Overflow		Application and Software	3
FILE-JAVA Oracle Java Private MethodHandle Sandbox Bypass	CVE-2013-5893	Application and Software	1
FILE-JAVA Sun Java Runtime Environment JPEGImageReader Heap Overflow		Application and Software	2
FILE-MULTIMEDIA	CVE-2008-	Multimedia	2

Apple QuickTime CVE-2008-1022 Obji Atom Parsing Stack Buffer Overflow	1088		
FILE-MULTIMEDIA Apple QuickTime FPX File Handling Integer Overflow	CVE-2006-1249	Multimedia	3
FILE-MULTIMEDIA MultiMedia Soft Components CVE-2009-0476 AdjMmsEng.dll PLS File Processing Buffer Overflow Attempt	CVE-2009-0476	Multimedia	1
FILE-MULTIMEDIA RealNetworks CVE-2007-5081 RealPlayer RealMedia File Format Processing Heap Corruption Attempt	CVE-2007-5081	Multimedia	2
FILE-MULTIMEDIA RealNetworks RealPlayer IVR Handling Heap Buffer Overflow		Multimedia	2
FILE-OFFICE Microsoft Excel CVE-2006-1306 Malformed OBJECT Record Code Execution	CVE-2006-1306	Office Tools	1
FILE-OFFICE Microsoft Excel CVE-2008-4019 REPT Function Integer Overflow	CVE-2008-4019	Office Tools	2
FILE-OFFICE Microsoft Excel CVE-2009-0238 Extrst Record Arbitrary	CVE-2009-0238	Office Tools	1

Code Excecution Attempt			
FILE-OFFICE Microsoft Excel Window2 Record Use After Free IV		Office Tools	1
FILE-OFFICE Microsoft Office Bad Index CVE-2014-6334 Memory Corruption (Published Exploit)	CVE-2014-6334	Office Tools	3
FILE-OFFICE Microsoft Office CVE-2007-1747 Drawing Object Code Execution	CVE-2007-1747	Office Tools	1
FILE-OFFICE Microsoft Office CVE-2012-1856 MSComctlLib.Toolbar ActiveX Control Exploit Attempt	CVE-2012-1856	Office Tools	1
FILE-OFFICE Microsoft Office CVE-2015-1649 RTF Out-Of-Bounds Array Access Remote Code Execution Attempt IV	CVE-2015-1649	Office Tools	2
FILE-OFFICE Microsoft Office CVE-2015-1649 RTF Out-Of-Bounds Array Access Remote Code Execution Attempt VII	CVE-2015-1649	Office Tools	2
FILE-OFFICE Microsoft Office CVE-2015-1649 RTF Out-Of-Bounds Array Access Remote Code Execution Attempt	CVE-2015-1649	Office Tools	2

V			
FILE-OFFICE Microsoft Office CVE-2015-1649 RTF Out-Of-Bounds Array Access Remote Code Execution Attempt X	CVE-2015-1649	Office Tools	2
FILE-OFFICE Microsoft Office CVE-2015-1683 File Modification Password Use After Free	CVE-2015-1683	Office Tools	2
FILE-OFFICE Microsoft Office CVE-2017-11826 OLEObject Type Confusion	CVE-2017-11826	Office Tools	1
FILE-OFFICE Microsoft Office Excel CVE-2010-0824 WOpt Record Memory Corruption Attempt II	CVE-2010-0824	Office Tools	2
FILE-OFFICE Microsoft Office Excel CVE-2010-0824 WOpt Record Memory Corruption Attempt I	CVE-2010-0824	Office Tools	2
FILE-OFFICE Microsoft Office Excel CVE-2011-1274 SerAuxTrend Biff Record Corruption Attempt	CVE-2011-1274	Office Tools	2
FILE-OFFICE Microsoft Office Excel CVE-2016-3284 empty bookViews element denial of service attempt	CVE-2016-3284	Office Tools	1

Vulnerability			
FILE-OFFICE Microsoft Office Outlook CVE-2006-1193 Web Access Script Injection Attempt	CVE-2006-1193	Office Tools	1
FILE-OFFICE Microsoft Office PowerPoint CVE-2009-0225 PP7 File Handling Memory Corruption	CVE-2009-0225	Office Tools	1
FILE-OFFICE Microsoft Outlook CVE-2004-0503 Object Security Bypass Vulnerability 1	CVE-2004-0503	Office Tools	2
FILE-OFFICE Microsoft Outlook CVE-2004-0503 Object Security Bypass Vulnerability 2	CVE-2004-0503	Office Tools	2
FILE-OFFICE Microsoft PowerPoint CVE-2016-3357 Bogus JPEG Marker Length Heap Buffer Overflow I	CVE-2016-3357	Office Tools	2
FILE-OFFICE Microsoft Visio CVE-2009-0097 Remote Code Execution	CVE-2009-0097	Office Tools	1
FILE-OFFICE Microsoft Windows CVE-2009-2506 WordPad and Office text converter integer overflow attempt	CVE-2009-2506	Office Tools	1
FILE-OFFICE Microsoft Word CVE-2018-0797	CVE-2018-0797	Office Tools	2

Memory Corruption Exploit Attempt			
FILE-OFFICE Soda PDF Insecure Library Loading	CVE-2013-3485	Office Tools	3
FILE-OTHER Adobe Acrobat CVE-2017-16395 EMF conversion heap buffer overflow attempt	CVE-2014-0529	Application and Software	2
FILE-OTHER Adobe Digital Editions CVE-2016-7889 Epub XXE Information Disclosure-II	CVE-2016-7889	Application and Software	2
FILE-OTHER Adobe Digital Editions CVE-2016-7889 Epub XXE Information Disclosure-I	CVE-2016-7889	Application and Software	2
FILE-OTHER ClamAV UPX File CVE-2013-2020 PE Parsing Memory Access Error	CVE-2013-2020	Application and Software	3
FILE-OTHER Corel PaintShop Pro Insecure Library Loading	CVE-2013-0733	Application and Software	2
FILE-OTHER ESTsoft ALZip MIM CVE-2011-1336 File Buffer Overflow Attempt	CVE-2011-1336	Application and Software	1
FILE-OTHER Interactive Data CVE-2011-3494 eSignal Stack Buffer Overflow	CVE-2011-3494	Application and Software	1

FILE-OTHER Microsoft Graphics CVE-2017-11763 Remote Code Execution Attempt	CVE-2017-11763	Application and Software	2
FILE-OTHER Microsoft Outlook Express CVE-2006-0014 Windows Address Book File Vulnerability	CVE-2006-0014	Application and Software	1
FILE-OTHER Microsoft Wordpad CVE-2013-3940 Embedded BMP Overflow Attempt	CVE-2013-3940	Application and Software	1
FILE-OTHER Oracle CVE-2012-0110 Outside In Lotus 1-2-3 Heap Overflow Attempt	CVE-2012-0110	Application and Software	1
FILE-OTHER Oracle Java SE CVE-2013-5907 GSUB ReqFeatureIndex Buffer Overflow Vulnerability	CVE-2013-5907	Application and Software	1
FILE-OTHER Sophos Anti-Virus CAB Files Invalid typeCompress Parsing Heap Buffer Overflow		Application and Software	1
FILE-OTHER Sophos Anti-Virus PDF Handling Stack Buffer Overflow		Application and Software	3
FILE-OTHER Sophos Anti-Virus RAR VMSF_DELTA Filter Signedness Error		Application and Software	2
FILE-OTHER Symantec	CVE-2016-	Application	2

Norton CVE-2016-2207 Antivirus ccScanw.dll Unpack ShortLZ memory corruption attempt	2207	and Software	
FILE-OTHER Trimble Navigation SketchUp CVE-2013-3664 BMP File Buffer Overflow	CVE-2013-3664	Application and Software	2
FILE-OTHER Unzip Extra Field CVE-2014-9636 Uncompressed Size Buffer Overflow II	CVE-2014-9636	Application and Software	2
FILE-OTHER Unzip Extra Field CVE-2014-9636 Uncompressed Size Buffer Overflow I	CVE-2014-9636	Application and Software	2
FILE-OTHER VMware CVE-2012-3569 OVF Tool Format String Vulnerability	CVE-2012-3569	Application and Software	2
FILE-PDF Adobe Acrobat and Reader CVE-2017-11254 addAnnot Use After Free Vulnerability		Application and Software	1
FILE-PDF Adobe Acrobat Reader CVE-2013-3346 Javascript Toolbar Button Use After Free Attempt	CVE-2013-3346	Application and Software	1
FILE-PDF Corel WordPerfect Document Processing Buffer Overflow III	CVE-2012-4900	Application and Software	3

FILE-PDF Microsoft Windows PDF Library Heap-based Buffer Overflow	CVE-2017-8728	Application and Software	1
MALWARE-CNC IoT Reaper botnet		Malware Communication	2
OS-LINUX cURL and libcurl CVE-2015-3145 Cookie Path Parsing Remote Code Execution	CVE-2015-3145	Operating System and Services	1
OS-LINUX Linux Kernel CVE-2004-0883 SMB Filesystem smb_proc_read Buffer Overflow	CVE-2004-0883	Operating System and Services	2
OS-SOLARIS Oracle Solaris RPC CVE-2017-3623 Heap Buffer Overflow	CVE-2017-3623	Operating System and Services	2
OS-WINDOWS Autodesk AutoCAD CVE-2014-0819 Insecure Library Loading	CVE-2014-0819	Operating System and Services	2
OS-WINDOWS Autodesk AutoCAD Insecure Library Loading	CVE-2014-0819	Operating System and Services	2
OS-WINDOWS Kerberos Multi-realm KDC NULL Pointer Dereference Denial of Service	CVE-2013-1418	Operating System and Services	3
OS-WINDOWS Microsoft FrontPage Server Extensions Cross	CVE-2006-0015	Operating System and Services	3

Site Scripting			
OS-WINDOWS Microsoft Graphics Component CREATECOLORSPACE Filesystem Information Disclosure	CVE-2016-0168	Operating System and Services	3
OS-WINDOWS Microsoft Hyperlink Object Library Information Disclosure	CVE-2016-0059	Operating System and Services	3
OS-WINDOWS Microsoft Malware Protection Engine File Processing Denial Of Service	CVE-2008-1437	Operating System and Services	2
OS-WINDOWS Microsoft .NET Framework CVE-2012-0015 Heap Corruption Vulnerability	CVE-2012-0015	Operating System and Services	2
OS-WINDOWS Microsoft .NET Framework CVE-2015-6115 ASLR Security Bypass	CVE-2015-6115	Operating System and Services	3
OS-WINDOWS Microsoft .NET Framework Remote Code Execution	CVE-2017-8759	Operating System and Services	1
OS-WINDOWS Microsoft Visual Studio CVE-2008-3704 MSMASK32.OCX ActiveX Control Buffer	CVE-2008-3704	Operating System and Services	2

Overflow			
OS-WINDOWS Microsoft Windows Active Directory CVE-2011-2014 LDAPS Authentication Bypass	CVE-2011-2014, reference:tsl,TSL20111108-07	Operating System and Services	3
OS-WINDOWS Microsoft Windows Common Controls MSCOMCTL.OCX Stack Buffer Overflow	CVE-2012-0158	Operating System and Services	2
OS-WINDOWS Microsoft Windows CVE-2010-3332 ASP.NET Information Disclosure Attempt II	CVE-2010-3332	Operating System and Services	3
OS-WINDOWS Microsoft Windows CVE-2010-3974 Fax Services Cover Page Editor Heap Buffer Overflow II	CVE-2010-3974	Operating System and Services	2
OS-WINDOWS Microsoft Windows CVE-2010-3974 Fax Services Cover Page Editor Heap Buffer Overflow I	CVE-2010-3974	Operating System and Services	2
OS-WINDOWS Microsoft Windows CVE-2013-3869 X.509 Certificate Validation Denial of Service	CVE-2013-3869	Operating System and Services	2
OS-WINDOWS Microsoft Windows CVE-2013-3900	CVE-2013-3900	Operating System and	1

WinVerifyTrust PE Validation Security Bypass		Services	
OS-WINDOWS Microsoft Windows CVE-2014-0315 File Handling Component Remote Code Execution II	CVE-2014-0315	Operating System and Services	1
OS-WINDOWS Microsoft Windows CVE-2014-0315 File Handling Component Remote Code Execution I	CVE-2014-0315	Operating System and Services	1
OS-WINDOWS Microsoft Windows CVE 2016-3393 Graphics engine EMF rendering vulnerability	CVE-2016-3393	Operating System and Services	1
OS-WINDOWS Microsoft Windows CVE-2017-0291 PDF Library JPEG2000 Parsing Out of Bounds Write	CVE-2017-0291	Operating System and Services	2
OS-WINDOWS Microsoft_Windows_Graphics_Component_CVE-2017-11816_Information_Disclosure	CVE-2016-3370	Operating System and Services	1
OS-WINDOWS Microsoft Windows Graphics CVE-2017-0190 META_SETDIBTODEV	CVE-2017-0190	Operating System and Services	1

Information Disclosure vulnerability			
OS-WINDOWS Microsoft Windows Imaging API Use After Free	CVE-2019-1311	Operating System and Services	1
OS-WINDOWS Microsoft Windows Indeo Codec Insecure Library Loading	CVE-2010-3138	Operating System and Services	2
OS-WINDOWS Microsoft Windows itss.dll CHM File Handling Heap Corruption (Published Exploit)	CVE-2006-2297	Operating System and Services	3
OS-WINDOWS Microsoft Windows LSASS Authenticate Message Denial of Service	CVE-2016-7237	Operating System and Services	3
OS-WINDOWS Microsoft Windows Media Format ASF Parsing Buffer Overflow	CVE-2006-4702	Operating System and Services	3
OS-WINDOWS Microsoft Windows Object Packager Remote Code Execution (Published Exploit)	CVE-2014-4114	Operating System and Services	3
OS-WINDOWS Microsoft Windows Object Packager Remote Code Execution	CVE-2014-4114	Operating System and Services	2

OS-WINDOWS Microsoft Windows OLE CVE-2016-0091 Code Execution	CVE-2016-0091	Operating System and Services	3
OS-WINDOWS Microsoft Windows Plug and Play Registry Key Access Buffer Overflow (MSRPC)	CVE-2005-2120	Operating System and Services	3
OS-WINDOWS Microsoft Windows Search CVE-2017-11771 Heap Buffer Overflow II	CVE-2017-11771	Operating System and Services	2
OS-WINDOWS Microsoft Windows SMB Authentication Reflection Remote Code Execution	CVE-2008-4037	Operating System and Services	1
OS-WINDOWS Microsoft Windows SMB OPEN2 Request Error Handling Memory Corruption	CVE-2008-4835	Operating System and Services	1
OS-WINDOWS Microsoft Windows SMB Server SMBv1 Out of Bounds Read	CVE-2017-11781	Operating System and Services	2
OS-WINDOWS Microsoft Windows SMB v1 CVE-2017-11772 Search Information Disclosure II	CVE-2017-11772	Operating System and Services	2
OS-WINDOWS Microsoft Windows	CVE-2017-8620	Operating System and	1

SMB v1 Search CVE-2017-8620 Type Confusion I		Services	
OS-WINDOWS Microsoft Windows SMB v2 CVE-2017-11772 Search Information Disclosure I	CVE-2017-11772	Operating System and Services	2
OS-WINDOWS Microsoft Windows SMB v2 Search CVE-2017-8620 Type Confusion II	CVE-2017-8620	Operating System and Services	1
OS-WINDOWS Microsoft Windows TrueType CVE-2012-4786 Font File Parsing Remote Code Execution	CVE-2012-4786	Operating System and Services	1
OS-WINDOWS Microsoft Windows VBScript Engine Information Disclosure	CVE-2015-6052	Operating System and Services	3
OS-WINDOWS Microsoft Windows WebDAV CVE-2012-0175 Invalid Character Argument Injection Attempt	CVE-2012-0175	Operating System and Services	2
OS-WINDOWS Microsoft XML Core Services parseError DOM Object Information Disclosure	CVE-2008-4029	Operating System and Services	3
OS-WINDOWS MIT Kerberos 5 build_principal_va	CVE-2015-2697	Operating System and	3

Denial of Service		Services	
OS-WINDOWS MIT Kerberos KDC Cross Realm Referral Denial of Service	CVE-2009-3295	Operating System and Services	3
OS-WINDOWS Oracle Java Runtime Environment Insecure File Loading		Operating System and Services	3
PROTOCOL-DNS Cesanta Mongoose CVE-2017-2909 DNS Compressed Name Denial of Service	CVE-2017-2909	DNS	2
PROTOCOL-DNS GNU C Library CVE-2015-1781 glibc getanswer_r Buffer Overflow Vulnerability	CVE-2015-1781	DNS	1
PROTOCOL-DNS ISC BIND ANY Query Response Assertion Failure Denial of Service	CVE-2016-9131	DNS	3
PROTOCOL-DNS ISC BIND DNS Cookie Assertion Failure Denial of Service	CVE-2016-2088	DNS	3
PROTOCOL-DNS ISC BIND rndc Control Channel Assertion Failure Denial of Service	CVE-2016-1285	DNS	3
PROTOCOL-DNS PowerDNS TKEY query denial of service	CVE-2015-5311	DNS	3

attempt			
PROTOCOL-DNS squid proxy CVE-2005-0446 Dns A Record Response Denial Of Service Attempt	CVE-2005-0446	DNS	3
PROTOCOL-DNS Tftpd32 DNS server denial of service attempt		DNS	1
PROTOCOL-DNS Tftpd32 DNS Server Denial Of Service Attempt		DNS	1
PROTOCOL-FTP Ipswitch WS_FTP Server FTP Commands Buffer Overflow	CVE-2006-4847	FTP	3
PROTOCOL-OTHER Git Client CVE-2014-9390 Path Validation Command Execution I	CVE-2014-9390	Operating System and Services	3
PROTOCOL-RPC nfs-utils CVE-2004-1014 TCP Connection Termination Denial of Service Vulnerability	CVE-2004-1014	Operating System and Services	1
PROTOCOL-RPC Rpcbind XDR CVE-2017-8779 Parsing Memory Exhaustion Denial of Service Vulnerability	CVE-2017-8779	Operating System and Services	1
PROTOCOL-RPC Rpcbind XDR Parsing Memory Exhaustion Denial of Service	CVE-2017-8779	Operating System and Services	1

PROTOCOL-SCADA Schneider Electric ClearSCADA OPF File Parsing Out of Bounds Array Indexing	CVE-2014-0779	Industrial Control System	3
PROTOCOL-SCADA Schneider Electric ProClima F1BookView Attach Memory Corruption	CVE-2015-7918	Industrial Control System	3
PROTOCOL-SNMP FreeBSD bsnmpd CVE-2014-1452 GETBULK PDU Stack Buffer Overflow Vulnerability	CVE-2014-1452	Operating System and Services	1
PROTOCOL-VOIP Digium Asterisk SIP Invalid SDP Media Descriptions Denial of Service (Published Exploit)	CVE-2013-5642	VoIP and Instant Messaging	2
SERVER-APACHE Apache 1.3 CVE-2004-0492 mod_proxy Buffer Overflow	CVE-2004-0492	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 CVE-2017-7659 HTTPD mod_http2 Null Pointer Dereference	CVE-2017-7659	Apache HTTP Server	2
SERVER-APACHE Apache httpd	CVE-2017-7668	Apache HTTP Server	2

ap_find_token Out of Bounds Read			
SERVER-APACHE Apache HTTPD CVE-2011-3368 mod_proxy Security Bypass I	CVE-2011-3368	Apache HTTP Server	3
SERVER-APACHE Apache HTTP Server CVE-2014-0098 mod_log_config Denial Of Service	CVE-2014-0098	Apache HTTP Server	1
SERVER-APACHE Apache HTTP Server CVE-2014-0118 mod_deflate Denial of Service	CVE-2014-0118	Apache HTTP Server	1
SERVER-APACHE Apache Input Header Folding CVE-2004-0493 Denial of Service Vulnerability	CVE-2004-0493	Apache HTTP Server	2
SERVER-APACHE Apache mod_imap and mod_imagemap Module Cross-Site Scripting	CVE-2007-5000	Apache HTTP Server	3
SERVER-APACHE Apache Solr CVE-2013-6397 SolrResourceLoader Directory Traversal	CVE-2013-6397	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 svn-ssh URL Command Execution	CVE-2017-9800	Apache HTTP Server	1
SERVER-APACHE Apache Tomcat Cookie Backslash Double Quotes Handling Information Disclosure	CVE-2012-0021	Apache HTTP Server	2
SERVER-APACHE Apache Tomcat CVE-2012-4534 NIO Connector Denial Of Service	CVE-2012-4534	Apache HTTP Server	3
SERVER-APACHE Apache Tomcat CVE-2013-4322 Large Chunked Transfer Denial Of Service	CVE-2013-4322	Apache HTTP Server	2
SERVER-IIS Microsoft IIS 7.5 CVE-2010-3229 Client Verify Null Pointer Attempt	CVE-2010-3229	Microsoft IIS web server	2
SERVER-MAIL Alt-N MDaemon File Attachment Directory Traversal Attempt		Other Mail Server	2
SERVER-MAIL BitDefender Antivirus CVE-2005-3154 Logging Function Format String Remote Code Execution Attempt	CVE-2005-3154	Other Mail Server	2
SERVER-MAIL Citadel SMTP RCPT TO Remote		Other Mail Server	1

Buffer Overflow			
SERVER-MAIL Exim CVE-2010-4344 string_format Remote Code Execution (Published Exploit)	CVE-2010-4344	Other Mail Server	1
SERVER-MAIL Exim Dovecot LDA Sender_Address Command Injection Attempt II		Other Mail Server	1
SERVER-MAIL Exim Dovecot LDA Sender_Address Command Injection Attempt I		Other Mail Server	1
SERVER-MAIL Exim With Dovecot LDA Sender_address Parameter Remote Command Execution		Other Mail Server	1
SERVER-MAIL IBM Domino IMAP Mailbox Name Stack Buffer Overflow	CVE-2017-1274	Other Mail Server	3
SERVER-MAIL Ipswitch IMail CVE-2006-4379 RCPT TO proxy overflow attempt	CVE-2006-4379	Other Mail Server	2
SERVER-MAIL Kinesphere CVE-2004-1945 eXchange POP3 Mail Server Overflow Attempt	CVE-2004-1945	Other Mail Server	2

SERVER-MAIL MailEnable IMAP Service EXAMINE and SELECT Commands Buffer Overflow (SELECT)		Other Mail Server	1
SERVER-MAIL Microsoft Exchange Server CVE-2007-0213 MIME base64 Decoding Code Execution Attempt	CVE-2007-0213	Other Mail Server	1
SERVER-MAIL Microsoft Office Outlook CVE-2008-2247 Web Access From Field Cross-Site Scripting	CVE-2008-2247	Other Mail Server	2
SERVER-MAIL Novell GroupWise Internet Agent CVE-2009-1636 Email Address Processing Buffer Overflow	CVE-2009-1636	Other Mail Server	1
SERVER-MAIL Novell Groupwise Internet Agent RCPT Command Overflow Attempt		Other Mail Server	1
SERVER-MAIL Symantec Brightmail AntiSpam Nested Zip Handling Denial Of Service Attempt		Other Mail Server	1
SERVER-ORACLE Oracle Database Server MD2 package VALIDATE GEOM procedure Buffer Overflow		Database Management System	2

SERVER-ORACLE Oracle Database Trigger MDSYS SDO_TOPO_DROP_FTBL SQL Injection Vulnerability	CVE-2008-3979	Database Management System	1
SERVER-OTHER Adobe ColdFusion CVE-2017-11284 RMI Registry Insecure Deserialization	CVE-2017-11284	Other Web Server	1
SERVER-OTHER Asterisk CVE-2017-16671 cdr_object_update_party_b_userfield_cb Buffer Overflow	CVE-2017-16671	Other Web Server	1
SERVER-OTHER EDB BrightStor ARCserve Backup Agent for MS SQL Server Buffer Overflow Vulnerability	CVE-2005-1272	Other Web Server	2
SERVER-OTHER Git CVE-2017-1000117 ssh URL Processing Command Execution Vulnerability	CVE-2017-1000117	Other Web Server	2
SERVER-OTHER HPE Operations Orchestration backwards-compatibility beanutils Insecure Deserialization	CVE-2017-8994	Other Web Server	1
SERVER-OTHER HP System Management CVE-2013-2362 Homepage iprange Stack Buffer Overflow	CVE-2013-2362	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 Tivoli Endpoint Manager CVE-2014-6140 Mobile Device Management Remote Code Execution Attempt	CVE-2014-6140	Other Web Server	2
SERVER-OTHER IBM Tivoli Provisioning Manager for OS Deployment CVE-2008-0401 HTTP Server Buffer Overflow	CVE-2008-0401	Other Web Server	1
SERVER-OTHER ISC BIND CVE-2015-4620 DNSSEC Validation Denial of Service	CVE-2015-4620	Other Web Server	2
SERVER-OTHER libsndfile PAF File Integer Overflow	CVE-2011-2696	Other Web Server	2
SERVER-OTHER McAfee ePolicy Orchestrator Framework Services Log Handling Format String Vulnerability	CVE-2008-1357	Other Web Server	3
SERVER-OTHER MIT Kerberos 5 Invalid RFC 1964 Token CVE-2014-4342 Denial of Service II	CVE-2014-4342	Other Web Server	1
SERVER-OTHER MIT Kerberos 5 Invalid RFC	CVE-2014-4342	Other Web Server	1

1964 Token CVE-2014-4342 Denial of Service I			
SERVER-OTHER MIT Kerberos 5 recvauth Invalid Memory Access	CVE-2014-5355	Other Web Server	2
SERVER-OTHER Nagios Remote Plugin Executor Command Injection		Other Web Server	2
SERVER-OTHER Network Time Protocol Daemon crypto-NAK Denial of Service	CVE-2016-4957	Other Web Server	3
SERVER-OTHER Network Time Protocol Daemon peer_xmit mode Denial of Service	CVE-2017-6464	Other Web Server	3
SERVER-OTHER Network Time Protocol Daemon read_mru_list Denial of Service	CVE-2016-7434	Other Web Server	3
SERVER-OTHER Novell eDirectory Unchecked Length Denial Of Service		Other Web Server	2
SERVER-OTHER Novell File Reporter CVE-2012-4956 VOL Tag Heap Buffer Overflow II	CVE-2012-4956	Other Web Server	1
SERVER-OTHER Novell iManager ASN.1 Parsing CVE-2003-0543 Denial of Service Vulnerability	CVE-2003-0543	Other Web Server	1
SERVER-OTHER Novell QuickFinder Server	CVE-2009-0611	Other Web Server	3

Multiple Cross Site Scripting			
SERVER-OTHER Novell ZENworks Configuration Management umaninv Information Disclosure	CVE-2013-1084	Other Web Server	3
SERVER-OTHER OpenLDAP rwm Overlay Denial of Service (Published Exploit)	CVE-2013-4449	Other Web Server	3
SERVER-OTHER OpenSSL AES-NI Integer Underflow (Published Exploit)	CVE-2012-2686	Other Web Server	3
SERVER-OTHER OpenSSL CVE-2012-2686 AES-NI Integer Underflow II	CVE-2012-2686	Other Web Server	2
SERVER-OTHER OpenSSL CVE-2012-2686 AES-NI Integer Underflow I	CVE-2012-2686	Other Web Server	2
SERVER-OTHER OpenSSL CVE-2013-6449 ssl_get_algorithm2 TLS Denial Of Service III	CVE-2013-6449	Other Web Server	2
SERVER-OTHER OpenSSL CVE-2013-6449 ssl_get_algorithm2 TLS Denial Of Service II	CVE-2013-6449	Other Web Server	2
SERVER-OTHER OpenSSL CVE-2013-	CVE-2013-6449	Other Web Server	2

6449 ssl_get_algorithm2 TLS Denial Of Service I			
SERVER-OTHER OpenSSL CVE 2014-0198 do_ssl3_write Denial of Service	CVE-2014-0198, reference:tsl,TSL20140505-01	Other Web Server	2
SERVER-OTHER OpenSSL CVE-2014-3569 ssl23_get_client_hello Function Denial of Service	CVE-2014-3569	Other Web Server	2
SERVER-OTHER OpenSSL CVE-2015-0291 ClientHello signature_algorithms Extension Denial of Service	CVE-2015-0291	Other Web Server	2
SERVER-OTHER OpenSSL CVE-2015-1793 Alternative Chains Certificate Forgery Policy Bypass	CVE-2015-1793	Other Web Server	1
SERVER-OTHER OpenSSL CVE-2016-6305 SSL_peek Infinite Loop Denial of Service	CVE-2016-6305	Other Web Server	1
SERVER-OTHER OpenSSL CVE-2016-6309 tls_get_message_body Function init_msg Structure Use After Free Vulnerability	CVE-2016-6309	Other Web Server	2

SERVER-OTHER OpenSSL CVE-2016-8610 SSL3_AL_WARNING Denial of Service	CVE-2016-8610	Other Web Server	1
SERVER-OTHER OpenSSL Invalid PSS Parameters Denial of Service	CVE-2015-0208	Other Web Server	3
SERVER-OTHER OpenSSL X509_cmp_time Denial of Service (Published Exploit)	CVE-2015-1789	Other Web Server	3
SERVER-OTHER Oracle CorelDRAW CVE-2013-0418 File Parser Heap Buffer Overflow Attempt	CVE-2013-0418	Other Web Server	1
SERVER-OTHER PHP CVE-2013-2110 Malformed Quoted Printable Denial Of Service Attempt	CVE-2013-2110	Other Web Server	2
SERVER-OTHER PHP CVE-2013-4248 SSL Certificate Validation Security Bypass II	CVE-2013-4248	Other Web Server	2
SERVER-OTHER PHP CVE-2013-4248 SSL Certificate Validation Security Bypass I	CVE-2013-4248	Other Web Server	2
SERVER-OTHER PHP exif_process_user_comment CVE-2016-6292	CVE-2016-6292	Other Web Server	3

Null Pointer Dereference II			
SERVER-OTHER Red Hat JBoss CVE-2013-6448 Seam InterfaceGenerator Information Disclosure Vulnerability	CVE-2013-6448	Other Web Server	1
SERVER-OTHER Samba CVE-2017-7494 Writeable Share Insecure Library Loading	CVE-2017-7494	Other Web Server	2
SERVER-OTHER Squid Proxy CVE-2007-6239 Cache Update Denial of Service	CVE-2007-6239	Other Web Server	1
SERVER-OTHER Squid Proxy ESI Component Stack Buffer Overflow	CVE-2016-4054	Other Web Server	3
SERVER-OTHER Squid Range Header Denial of Service	CVE-2014-3609	Other Web Server	3
SERVER-OTHER Squid Squoison CVE-2016-4553 Host Header Cache Poisoning	CVE-2016-4553	Other Web Server	3
SERVER-OTHER Squid SSL-Bump Denial Of Service II		Other Web Server	2
SERVER-OTHER Squid SSL-Bump Denial Of Service I		Other Web Server	2
SERVER-OTHER	CVE-2012-	Other Web	2

Symantec Messaging Gateway CVE-2012-3579 Default SSH Password	3579	Server	
SERVER-SAMBA Samba CVE-2015-5252 smbd Daemon Symlink Verification Information Disclosure	CVE-2015-5252	Operating System and Services	3
SERVER-SAMBA Samba Root File System Access Security Bypass	CVE-2009-0022	Operating System and Services	3
SERVER-SAMBA Samba SMB1 smb_request_done Use After Free	CVE-2017-14746	Operating System and Services	3
SERVER-SAMBA Samba smbd read_nttrans_ea_list Infinite Allocation Loop Denial of Service	CVE-2013-4124	Operating System and Services	3
SERVER-WEBAPP 1999-0070		Web Services and Applications	1
SERVER-WEBAPP AlienVault CVE-2014-3805 OSSIM av-centerd Util.pm get_license Arbitrary Command Execution	CVE-2014-3805	Web Services and Applications	1
SERVER-WEBAPP Alienvault CVE-2016-8582 Unified Security Management and OSSIM gauge.php SQL	CVE-2016-8582	Web Services and Applications	2

Injection			
SERVER-WEBAPP AlienVault Unified Security Management av-forward Deserialization Remote Code Execution		Web Services and Applications	2
SERVER-WEBAPP Apache Jetspeed PageManagementServic e Cross-Site Scripting	CVE-2016-0711	Web Services and Applications	3
SERVER-WEBAPP Apache Tomcat Directory Listing Information Disclosure		Web Services and Applications	2
SERVER-WEBAPP Apple Products CVE-2014-1266 SSLVerifySignedServerK eyExchange Security Feature Bypass Vulnerability	CVE-2014-1266	Web Services and Applications	1
SERVER-WEBAPP Apple Products SSLVerifySignedServerK eyExchange Security Feature Bypass Vulnerability	CVE-2014-1266	Web Services and Applications	1
SERVER-WEBAPP Brocade Network Advisor SoftwareImageUpload name filename Directory Traversal	CVE-2016-8206	Web Services and Applications	3
SERVER-WEBAPP Cacti spikekill.php Cross-Site	CVE-2017-	Web Services and	2

Scripting	12927	Applications	
SERVER-WEBAPP EMC CMCNE inmservlets.war FileUploadController Arbitrary File Upload	CVE-2013-6810	Web Services and Applications	3
SERVER-WEBAPP Endian Firewall CVE-2015-5082 Proxy Password Change Command Execution	CVE-2015-5082	Web Services and Applications	3
SERVER-WEBAPP Exim Buffer Overflows	CVE-2004-0399	Web Services and Applications	2
SERVER-WEBAPP Exponent CVE-2017-7991 CMS eaasController.php api Function SQL Injection	CVE-2017-7991	Web Services and Applications	1
SERVER-WEBAPP GnuTLS Server Hello Session ID Heap Buffer Overflow	CVE-2014-3466	Web Services and Applications	2
SERVER-WEBAPP HPE Intelligent Management Center CVE-2017-12559 mibFileServlet file Directory Traversal	CVE-2017-12559	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 HP Intelligent Management Center img Buffer Overflow		Web Services and Applications	1

SERVER-WEBAPP IBM Lotus Notes CVE-2005-2175 Cross Site Scripting	CVE-2005-2175	Web Services and Applications	2
SERVER-WEBAPP ManageEngine CVE-2014-6037 EventLog Analyzer agentUpload Directory Traversal	CVE-2014-6037	Web Services and Applications	1
SERVER-WEBAPP McAfee ePolicy CVE-2015-0921 Orchestrator XML Entity Injection	CVE-2015-0921	Web Services and Applications	2
SERVER-WEBAPP McAfee Firewall Reporter isValidClient Remote Code Execution		Web Services and Applications	1
SERVER-WEBAPP NagiosQL txtSearch Parameter Cross-Site Scripting	CVE-2013-6039	Web Services and Applications	3
SERVER-WEBAPP Novell CVE-2013-1080 ZENworks Configuration Management File Upload	CVE-2013-1080	Web Services and Applications	2
SERVER-WEBAPP Novell File Reporter CVE-2012-4957 SRS Arbitrary File Retrieval	CVE-2012-4957	Web Services and Applications	2
SERVER-WEBAPP Novell File Reporter SRS Arbitrary File Retrieval	CVE-2012-4957	Web Services and Applications	3
SERVER-WEBAPP Novell	CVE-2013-	Web Services	2

ZENworks Configuration Management CVE-2013-1080 File Upload II	1080	and Applications	
SERVER-WEBAPP Novell ZENworks Configuration Management CVE-2013-1080 File Upload I	CVE-2013-1080	Web Services and Applications	2
SERVER-WEBAPP op5 Monitor command_test.php Command Injection		Web Services and Applications	2
SERVER-WEBAPP Oracle GlassFish Enterprise Server CVE-2012-0550 REST Interface Cross Site Request Forgery	CVE-2012-0550	Web Services and Applications	2
SERVER-WEBAPP Oracle Identity Manager CVE-2017-10151 Default Credentials II	CVE-2017-10151	Web Services and Applications	3
SERVER-WEBAPP Oracle Identity Manager CVE-2017-10151 Default Credentials I	CVE-2017-10151	Web Services and Applications	1
SERVER-WEBAPP Oracle Warehouse Builder CVE-2011-0799 WB_RT_AUDIT_SHADOW_TABLE Multiple SQL Injections	CVE-2011-0799	Web Services and Applications	2
SERVER-WEBAPP Oracle WebLogic Server CVE-2010-4437 Session Fixation I	CVE-2010-4437	Web Services and Applications	1

SERVER-WEBAPP PHP CVE-2013-4113 xml_parse_into_struct Heap Memory Corruption	CVE-2013-4113	Web Services and Applications	2
SERVER-WEBAPP PHPMailer CVE-2016-10033 Mail Sender Command Injection I	CVE-2016-10033	Web Services and Applications	2
SERVER-WEBAPP PHP phar_parse_pharfile Function filename_len Property Integer Overflow	CVE-2016-10159	Web Services and Applications	3
SERVER-WEBAPP PHP SdnToJewish Function Integer Overflow Vulnerability	CVE-2013-4635	Web Services and Applications	1
SERVER-WEBAPP Red Hat JBoss Seam Framework XXE Information Disclosure	CVE-2013-6447	Web Services and Applications	3
SERVER-WEBAPP Schneider Electric SCADA Expert CVE-2014-5411 ClearSCADA Denial of Service Vulnerability	CVE-2014-5411	Web Services and Applications	1
SERVER-WEBAPP SERVER_WEBAPP Novell CVE-2013-1080 ZENworks Configuration Management File Upload	CVE-2013-1080	Web Services and Applications	2
SERVER-WEBAPP		Web Services	1

Sophos Web Appliance change_password Admin Password Privilege Escalation		and Applications	
SERVER-WEBAPP Symantec CVE-2012-2574 Web Gateway blocked.php Blind SQL Injection	CVE-2012-2574	Web Services and Applications	1
SERVER-WEBAPP Symantec Endpoint CVE-2016-3652 Protection Manager Cross-Site Scripting II	CVE-2016-3652	Web Services and Applications	2
SERVER-WEBAPP Symantec Web Gateway dbutils.php SQL Injection	CVE-2014-1651	Web Services and Applications	3
SERVER-WEBAPP Trend Micro InterScan Messaging Security modTMCSS Command Injection (Decrypted Traffic)	CVE-2017-11391	Web Services and Applications	3
SERVER-WEBAPP Trend Micro InterScan Messaging Security modTMCSS Command Injection	CVE-2017-11391	Web Services and Applications	3
SERVER-WEBAPP Trend Micro IWSVA domains Command Injection III		Web Services and Applications	2
SERVER-WEBAPP Trend Micro IWSVA domains Command Injection II		Web Services and Applications	2

SERVER-WEBAPP Trend Micro IWSVA domains Command Injection I		Web Services and Applications	2
SERVER-WEBAPP Trend Micro IWSVA LogSettingHandler doPostMountDevice Command Injection		Web Services and Applications	2
SERVER-WEBAPP Trend Micro IWSVA ManageSRouteSettings HttpServlet Command Injection		Web Services and Applications	2
SERVER-WEBAPP Trend Micro IWSVA ReportHandler DoCmd Command Injection		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 SafeSync for Enterprise replace_local_disk Command Injection (Decrypted Traffic)		Web Services and Applications	1
SERVER-WEBAPP Trend Micro SafeSync for Enterprise replace_local_disk Command Injection		Web Services and Applications	1

SERVER-WEBAPP Trend Micro Smart Protection Server wcs_bwlists_handler.php Command Injection		Web Services and Applications	2
SERVER-WEBAPP Typo3 CMS CVE-2015-5956 show_rechis Cross Site Scripting Attempt II	CVE-2015-5956	Web Services and Applications	1
SERVER-WEBAPP Typo3 CMS CVE-2015-5956 show_rechis Cross Site Scripting Attempt I	CVE-2015-5956	Web Services and Applications	1
SERVER-WEBAPP Webmin show.cgi Command Execution	CVE-2012-2982	Web Services and Applications	3
SERVER-WEBAPP Zabbix Server CVE-2017-2824 Active Proxy Trapper Command Injection II	CVE-2017-2824	Web Services and Applications	1
SERVER-WEBAPP Zabbix Server CVE-2017-2824 Active Proxy Trapper Command Injection I	CVE-2017-2824	Web Services and Applications	1
SERVER-WEBAPP Zenoss CVE-2014-6261 Core Version Check Remote Code Execution II	CVE-2014-6261	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

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