SOPHOS
Security made simple.

SOPHOS
IPS Signature Update
Release Notes

Version: 9.16.15

Release Date : 01st August 2019

Release Information

Upgrade Applicable on

IPS Signature Release	Version 9.16.14
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 9.16.15 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.

The table below provides details of signatures included in this release.

This IPS Release includes One Hundred and Eighteen(118) signatures to address Eighty Nine(89) vulnerabilities.

New signatures are added for the following vulnerabilities:

Name	CVE–ID	Category	Severity
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-IE Microsoft Internet Explorer 11 VBScript Execution Policy Bypass	CVE-2019-0768	Browsers	2
BROWSER-PLUGINS IBM SPSS SamplePower ActiveX clsid access attempt	CVE-2012-5945	Browsers	2
FILE-FLASH Adobe Acrobat Flash Player request for atl.dll over SMB attempt	CVE-2012-0756	Multimedia	2
FILE-FLASH Adobe Acrobat Flash Player request for uxtheme.dll over SMB attempt	CVE-2012-0756	Multimedia	2
FILE-FLASH Adobe Flash Player malformed ATF heap overflow attempt	CVE-2016-1002	Multimedia	2

FILE-FLASH Adobe Flash Player null pointer dereference attempt	CVE-2011-0626	Multimedia	2
FILE-FLASH Adobe Flash Player request for apphelp.dll over SMB attempt	CVE-2016-4140	Multimedia	2
FILE-FLASH Adobe Flash Player request for ClbCatQ.dll over SMB attempt	CVE-2016-1014	Multimedia	2
FILE-FLASH Adobe Flash Player request for dbghelp.dll over SMB attempt	CVE-2016-4140	Multimedia	2
FILE-FLASH Adobe Flash Player request for HNetCfg.dll over SMB attempt	CVE-2016-1014	Multimedia	2
FILE-FLASH Adobe Flash Player request for MSIMG32.dll over SMB attempt	CVE-2016-4116	Multimedia	2
FILE-FLASH Adobe Flash Player request for RASMan.dll over SMB attempt	CVE-2016-1014	Multimedia	2
FILE-FLASH Adobe Flash Player request for setupapi.dll over SMB attempt	CVE-2016-1014	Multimedia	2
FILE-FLASH Microsoft Internet Explorer premature unload of	CVE-2012-5272	Multimedia	2

Flash plugin use after free attempt			
FILE-IMAGE Directshow GIF logical height overflow attempt	CVE-2013-3174	Multimedia	2
FILE-IMAGE Directshow GIF logical width overflow attempt	CVE-2013-3174	Multimedia	2
FILE-OFFICE Microsoft Access remote code execution attempt	CVE-2018-0903	Office Tools	1
FILE-OFFICE Microsoft Office Access Jet Database Engine integer overflow attempt	CVE-2017-0250	Office Tools	2
FILE-OFFICE Microsoft Office Excel ObjBiff exploit attempt	CVE-2011-1272	Office Tools	2
FILE-OFFICE Microsoft Office Excel with embedded Flash file attachment attempt	NA	Office Tools	2
FILE-OFFICE Microsoft Office request for api-ms-win-core-winrt-l1-1-0.dll over SMB attempt	CVE-2016-0018	Office Tools	2
FILE-OFFICE Microsoft Office request for elsext.dll over SMB attempt	CVE-2015-6128	Office Tools	2
FILE-OFFICE Microsoft Office request for mfplat.dll over SMB	CVE-2016-0016	Office Tools	3

attempt			
FILE-OFFICE Microsoft Office request for mqrt.dll over SMB attempt	CVE-2015-6132	Office Tools	3
FILE-OFFICE Microsoft Office request for msdaora.dll over SMB attempt	CVE-2016-0041	Office Tools	3
FILE-OFFICE Microsoft Office request for phoneinfo.dll over SMB attempt	CVE-2016-0041	Office Tools	2
FILE-OFFICE Microsoft Office Word document malicious lcbSttbfBkmkArto value attempt	CVE-2014-6333	Office Tools	2
FILE-OFFICE Microsoft Office Word Out-of-Bounds Write attempt	CVE-2017-0003	Office Tools	2
FILE-OFFICE Microsoft Office Word request for OLMAPI32.dll over SMB attempt	CVE-2016-0042	Office Tools	3
FILE-OFFICE Microsoft Office wwlib out of bounds memory access attempt	CVE-2016-0183	Office Tools	2
FILE-OFFICE Microsoft Windows common controls MSCOMCTL.OCX buffer overflow attempt	CVE-2012-0158	Office Tools	2

FILE-OTHER Adobe Acrobat Pro TIFF embedded XPS file out of bounds read attempt	CVE-2018-4903	Application and Software	2
FILE-OTHER Adobe Acrobat Reader plugin ace.dll dll-load exploit attempt	CVE-2011-0570	Application and Software	2
FILE-OTHER Adobe Acrobat request for updaternotifications.dll over SMB attempt	CVE-2016-1008	Application and Software	2
FILE-OTHER Adobe Photoshop request for wintab32.dll over SMB attempt	CVE-2010-3127	Application and Software	2
FILE-OTHER Apple OSX ZIP archive shell script execution attempt	CVE-2006-0848	Application and Software	2
FILE-OTHER Microsoft System.Uri heap corruption attempt	CVE-2014-4121	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 device metadata file directory traversal attempt	NA	Application and Software	2
FILE-OTHER Microsoft Windows GDI32.dll cmap numUVSMappings	CVE-2016-7274	Application and Software	2

overflow attempt			
FILE-OTHER Microsoft Windows Media Center link file code execution attempt	CVE-2015-2509	Application and Software	2
FILE-OTHER Microsoft Windows VBScript Engine VbsErase Memory Corruption	CVE-2019-0667	Application and Software	2
FILE-OTHER Microsoft Wordpad embedded BMP overflow attempt	CVE-2013-3940	Application and Software	2
FILE-OTHER multiple products malformed CUE file buffer overflow attempt	CVE-2007-2888	Application and Software	2
FILE-OTHER Multiple products request for dwmapi.dll over SMB attempt	CVE-2010-3127	Application and Software	3
FILE-OTHER Multiple products request for version.dll over SMB attempt	CVE-2012-0756	Multimedia	3
FILE-OTHER Multiple products version.dll dll-load exploit attempt	CVE-2012-0756	Multimedia	2
FILE-OTHER RealNetworks RealPlayer RMP file heap buffer overflow attempt	CVE-2013-6877	Application and Software	2
FILE-PDF Adobe Acrobat	CVE-	Application and	2

Reader malformed TTF buffer over-read attempt	2017-16365	Software	
FILE-PDF Adobe Acrobat Reader malformed UTF-16 string memory corruption attempt	CVE-2017-11236	Application and Software	2
FILE-PDF malformed embedded JPEG2000 image information disclosure attempt	CVE-2017-16374	Application and Software	2
MALWARE-CNC Dharma ransomware dropper initial outbound connection	NA	Malware Communication	1
MALWARE-CNC Dharma ransomware dropper outbound connection	NA	Malware Communication	1
MALWARE-CNC Linux.Downloader.Mumblehard variant outbound connection	NA	Malware Communication	2
MALWARE-CNC Unix.Trojan.Mirai variant post compromise download attempt	NA	Malware Communication	2
MALWARE-CNC Unix.Trojan.Mirai variant post compromise download	NA	Malware Communication	4
MALWARE-CNC Unix.Trojan.Vpnfilter variant SSL connection	NA	Malware Communication	2

attempt			
MALWARE-CNC User-Agent known malicious user-agent string - Sality	NA	Malware Communication	2
OS-LINUX Linux Kernel Netfilter iptables-restore Stack-based Buffer Overflow	CVE-2019-11360	Operating System and Services	2
OS-LINUX Linux kernel SCTP duplicate cookie denial of service attempt	CVE-2013-2206	Operating System and Services	1
OS-OTHER x86 FreeBSD overflow attempt	NA	Operating System and Services	2
OS-WINDOWS DCERPC ISystemActivate flood attempt	CVE-2003-0813	Operating System and Services	2
OS-WINDOWS Microsoft Expression Design request for wintab32.dll over SMB attempt	CVE-2012-0016	Operating System and Services	3
OS-WINDOWS Microsoft Lync Online request for ncrypt.dll over SMB attempt	CVE-2012-1849	Operating System and Services	3
OS-WINDOWS Microsoft product request for fputlsat.dll over SMB attempt	CVE-2011-0029	Operating System and Services	3
OS-WINDOWS Microsoft Windows Cinepak Codec Code	CVE-2010-2553	Operating System and Services	2

Execution			
OS-WINDOWS Microsoft Windows Cinepak Codec Code Execution	CVE-2010-2553	Operating System and Services	4
OS-WINDOWS Microsoft Windows Encrypted DCERPC request attempt	NA	Operating System and Services	3
OS-WINDOWS Microsoft Windows RDP RST denial of service attempt	CVE-2012-0152	Operating System and Services	1
OS-WINDOWS Microsoft Windows request for feclient.dll over SMB attempt	CVE-2016-0014	Operating System and Services	2
OS-WINDOWS Microsoft Windows Shell Handler remote code execution attempt	CVE-2010-0027	Operating System and Services	1
OS-WINDOWS Microsoft Windows SMB large NT RENAME transaction request memory leak attempt	NA	Operating System and Services	2
OS-WINDOWS Microsoft Windows WINS internal communications on network exploit attempt	CVE-2011-1984	Operating System and Services	2
PROTOCOL-DNS dnsmasq add_pseudoheader	CVE-2017-14495	DNS	2

memory leak attempt			
PROTOCOL-DNS excessive queries of type ANY - potential DoS	NA	DNS	1
PROTOCOL-DNS ISC BIND recursive resolver resource consumption denial of service attempt	CVE-2014-8500	DNS	2
PROTOCOL-IMAP login brute force attempt	NA	Operating System and Services	3
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 dhcpcd DHCPv6 CVE-2019-11577 dhcp6_findna Buffer Overflow	CVE-2019-11577	Other Web Server	2
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 NTPsec ntpd write_variables Denial of Service	CVE-2019-6445	Other Web Server	2

SERVER-OTHER RARLAB WinRAR ACE Directory Traversal	CVE-2018-20251	Other Web Server	2
SERVER-OTHER RARLAB WinRAR ACE Directory Traversal	CVE-2018-20251	Other Web Server	4
SERVER-OTHER Red Hat librelp Stack Buffer Overflow	CVE-2018-1000140	Other Web Server	2
SERVER-WEBAPP Zoho ManageEngine OpManager BusinessViewFlashImpl handleBVAction XXE Injection	CVE-2018-18980	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