SOPHOS
Security made simple.

SOPHOS
IPS Signature Update
Release Notes

Version : 9.18.77

Release Date : 09th December 2021

Release Information

Upgrade Applicable on

IPS Signature Release	Version 9.18.76
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 9.18.77 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 Sixty Two(62) signatures to address Fifty Eight(58) vulnerabilities.

New signatures are added for the following vulnerabilities:

Name	CVE–ID	Category	Severity
BROWSER-IE Microsoft Internet Explorer drag event memory corruption attempt	CVE-2011-1254	browser-ie	1
BROWSER-IE Microsoft Internet Explorer uninitialized or deleted object access attempt	CVE-2009-2530	browser-ie	1
BROWSER-OTHER WGet symlink arbitrary file write attempt	CVE-2014-4877	browser-other	1
FILE-FLASH Adobe Flash Player AVM domain memory range integer overflow attempt	CVE-2015-8651	file-flash	1
FILE-FLASH Adobe Flash Player null pointer dereference attempt	CVE-2011-0626	file-flash	2
FILE-IDENTIFY AVI Video file magic detected		file-identify	4
FILE-MULTIMEDIA Microsoft Windows Media Player JPG header record mismatch memory corruption attempt	CVE-2010-1880	file-multimedia	1
FILE-MULTIMEDIA VideoLAN VLC Media Player MMS Plugin CVE-2012-1775 Stack Buffer	CVE-2012-1775	file-multimedia	3

Overflow			
FILE-OFFICE Microsoft Office Excel ShrFmla record use after free attempt	CVE-2011-1986	file-office	1
FILE-OFFICE Microsoft Office Excel SXLI record integer overrun attempt	CVE-2012-0184	file-office	1
FILE-OFFICE Microsoft Office GDI library TIFF handling integer overflow attempt	CVE-2013-3906	file-office	1
FILE-OFFICE Microsoft Office PowerPoint pp4x322.dll dll-load exploit attempt	CVE-2011-3396	file-office	1
FILE-OFFICE Microsoft Office pptimpconv.dll dll-load exploit attempt	CVE-2010-3337	file-office	1
FILE-OFFICE Microsoft Office Word CVE-2014-6334 fcPlfguidUim out-of-bounds attempt	CVE-2014-6334	file-office	1
FILE-OFFICE Microsoft Word malformed css remote code execution attempt	CVE-2008-1434	file-office	1
FILE-OTHER Adobe Premiere Pro ibfs32.dll dll-load exploit attempt	CVE-2010-3150	file-other	1
FILE-PDF Adobe Acrobat file extension overflow attempt	CVE-2004-0632	file-pdf	2

FILE-PDF Adobe Acrobat Reader JpxDecode invalid crgn memory corruption attempt	CVE-2009-3955	file-pdf	1
FILE-PDF Adobe Acrobat Reader mishandling of invalid triangle edge access attempt	CVE-2014-8459	file-pdf	1
FILE-PDF Adobe Acrobat Reader TTF SING table parsing remote code execution attempt	CVE-2010-2883	file-pdf	1
MALWARE-CNC Mirai Botnet Attack Attempt		malware-cnc	1
MALWARE-CNC Win.Trojan.CryptoWall variant outbound connection		malware-cnc	2
MISC ROWSER-PLUGINS SAP 3D Visual Enterprise Viewer 3DM File Buffer Overflow		misc	1
OS-MOBILE Adobe Reader Mobile CVE-2014-0514 JavaScript Interface Java Code Execution	CVE-2014-0514	os-mobile	1
OS-MOBILE Android/Nickispy.D sms logging request detection		os-mobile	1
OS-SOLARIS Oracle Solaris DHCP Client CVE-2005-2870 Arbitrary	CVE-2005-2870	os-solaris	2

Code Execution attempt			
OS-WINDOWS CAB SIP authenticode alteration attempt	CVE-2010-0487	os-windows	1
OS-WINDOWS Microsoft Color Control Panel STI.dll dll-load exploit attempt	CVE-2010-5082	os-windows	1
OS-WINDOWS Microsoft Groove mso.dll dll-load exploit attempt	CVE-2010-3146	os-windows	1
OS-WINDOWS Microsoft Lync Online request for ncrypt.dll over SMB attempt	CVE-2012-1849	os-windows	3
OS-WINDOWS Microsoft Windows NtCreateTransactionManager type confusion attempt	CVE-2015-1643	os-windows	2
OS-WINDOWS Microsoft Windows Print Spooler arbitrary file write attempt	CVE-2010-2729	os-windows	1
OS-WINDOWS Microsoft Windows shell extensions deskpan.dll dll-load exploit attempt	CVE-2011-1991	os-windows	1
OS-WINDOWS Microsoft Windows SMB Negotiate Protocol response DoS attempt -	CVE-2009-3676	os-windows	2

empty SMB 2			
PROTOCOL-NNTP Microsoft Windows SEARCH pattern overflow attempt	CVE-2004-0574	protocol-nntp	1
PROTOCOL-SNMP HP Huawei password disclosure attempt	CVE-2012-3268	protocol-snmp	2
SCAN Nuclei Vulnerability Scanner		scan	3
SCAN Zgrab Scanning Attempt Detected		scan	3
SCAN ZmEu Vulnerability Scanner		scan	3
SERVER-APACHE Apache Killer denial of service tool exploit attempt	CVE-2011-3192	server-apache	2
SERVER-IIS adctest.asp access		server-iis	1
SERVER-IIS MSProxy access		server-iis	1
SERVER-OTHER Free Software Foundation GnuTLS record application integer overflow attempt	CVE-2012-1573	server-other	3
SERVER-OTHER HP Diagnostics Server magentservice.exe stack overflow attempt	CVE-2011-4789	server-other	1
SERVER-OTHER		server-other	1

Microsoft Frontpage service.pwd			
SERVER-OTHER Microsoft Frontpage services.cnf access	CVE-2002-1717	server-other	3
SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	CVE-2014-0160	server-other	3
SERVER-OTHER Oracle Java Applet2ClassLoader Remote Code Execution	CVE-2010-4452	server-other	1
SERVER-OTHER PHP unserialize use after free attempt	CVE-2014-8142	server-other	2
SERVER-WEBAPP Blahz-DNS dostuff.php modify user attempt	CVE-2002-0599	server-webapp	1
SERVER-WEBAPP HP OpenView Network Node Manager ovet_demandpoll.exe format string execution attempt	CVE-2010-1550	server-webapp	1
SERVER-WEBAPP HP OpenView NNM getnnmdata.exe CGI hostname parameter buffer overflow attempt	CVE-2010-1555	server-webapp	1
SERVER-WEBAPP HP OpenView NNM ovwebsnmpsrv.exe command line	CVE-2010-1960	server-webapp	1

argument buffer overflow attempt			
SERVER-WEBAPP HP OpenView NNM snmpviewer.exe CGI parameter buffer overflow attempt	CVE-2010-1552	server-webapp	1
SERVER-WEBAPP HP OpenView NNM webappmon.exe buffer overflow attempt	CVE-2010-2703	server-webapp	1
SERVER-WEBAPP HP OpenView Performance Insight Server backdoor account code execution attempt	CVE-2011-0276	server-webapp	1
SERVER-WEBAPP Lizard Cart CMS SQL injection in detail.php id attempt	CVE-2006-0087	server-webapp	2
SERVER-WEBAPP SkyBlueCanvas CMS contact page command injection attempt	CVE-2014-1683	server-webapp	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	Critical
2	Major
3	Moderate
4	Minor
5	Warning

Important Notice

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

RESTRICTED RIGHTS

Corporate Headquarters

Sophos Technologies Pvt. Ltd.
Registered in England and Wales No. 2096520,
The Pentagon, Abingdon Science Park,
Abingdon, OX14 3YP, UK
Web site: www.sophos.com