SOPHOS
Security made simple.

SOPHOS
IPS Signature Update
Release Notes

Version : 9.17.46
Release Date : 17th September 2020

Release Information

Upgrade Applicable on

IPS Signature Release	Version 9.17.45
Sophos Appliance Models	CR250i, CR300i, CR500i-4P, CR500i-6P, CR500i-8P, CR500ia, CR500ia-RP, CR500ia1F, CR500ia10F, CR750ia, CR750ia1F, CR750ia10F, CR1000i-11P, CR1000i-12P, CR1000ia, CR1000ia10F, CR1500i-11P, CR1500i-12P, CR1500ia, CR1500ia10F CR25iNG, CR25iNG-6P, CR35iNG, CR50iNG, CR100iNG, CR200iNG/XP, CR300iNG/XP, CR500iNG-XP, CR750iNG-XP, CR2500iNG, CR25wiNG, CR25wiNG-6P, CR35wiNG, CRiV1C, CRiV2C, CRiV4C, CRiV8C, CRiV12C, XG85 to XG450, SG105 to SG650

Upgrade Information

Upgrade type: Automatic

Compatibility Annotations: None

Introduction

The Release Note document for IPS Signature Database Version 9.17.46 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 Eighteen(18) signatures to address Sixteen(16) vulnerabilities.

New signatures are added for the following vulnerabilities:

Name	CVE–ID	Category	Severity
BROWSER-PLUGINS Advantech Webaccess webvrpcs Directory Traversal Remote Code Execution CVE-2017-16720	CVE-2017-16720	Browsers	1
FILE-OTHER IBM Installation Manager iim URI Handling Code Execution		Application and Software	1
FILE-OTHER Microsoft Windows CVE-2016-7256 OTF Parsing Memory Corruption	CVE-2016-7256	Application and Software	1
FILE-OTHER Microsoft Windows CVE-2016-7274 GDI32.dll cmap numUVSMappings overflow attempt vulnerabilty	CVE-2016-7274	Application and Software	1
OS-WINDOWS Microsoft Windows Netlogon crafted NetrServerAuthenticate or NetrServerPasswordSet elevation of privilege attempt	CVE-2020-1472	Operating System and Services	1
OS-WINDOWS Microsoft Windows Netlogon crafted NetrServerReqChalleng	CVE-2020-1472	Operating System and Services	1

e elevation of privilege attempt			
OS-WINDOWS Windows Netlogon Elevation of Privilege Vulnerability		Operating System and Services	1
SERVER-OTHER HP Data Protector CRS Multiple Opcodes Stack Buffer Overflow	CVE-2013-2324	Other Web Server	1
SERVER-OTHER HP Data Protector CRS Multiple Stack Buffer Overflows	CVE-2013-6195	Other Web Server	1
SERVER-OTHER HP Intelligent Management Center dbman CVE-2017-5820 BackupZipFile opcode command injection Vulnerability	CVE-2017-5820	Other Web Server	1
SERVER-OTHER HP Network Node Manager I ovopi.dll -D Buffer Overflow	CVE-2014-2624	Other Web Server	2
SERVER-OTHER HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution	CVE-2011-0269	Other Web Server	1
SERVER-OTHER HP OpenView Network Node Manager ovalarmsrv Integer Overflow	CVE-2008-2438	Other Web Server	1

SERVER-OTHER HP Power Manager Remote Code Execution	CVE-2009-2685	Other Web Server	1
SERVER-OTHER HPE Data Protector EXEC_BAR username Buffer Overflow	CVE-2016-2005	Other Web Server	1
SERVER-OTHER Lotus Domino LDAP Heap Buffer Overflow Attempt	CVE-2010-0358	Other Web Server	1

- **Name:** Name of the Signature

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

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

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

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

Important Notice

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

RESTRICTED RIGHTS

Corporate Headquarters

Sophos Technologies Pvt. Ltd.

Registered in England and Wales No. 2096520,

The Pentagon, Abingdon Science Park,

Abingdon, OX14 3YP, UK

Web site: www.sophos.com