SOPHOS
Security made simple.

SOPHOS
IPS Signature Update
Release Notes

Version : 9.17.45
Release Date : 16th September 2020

Release Information

Upgrade Applicable on

IPS Signature Release	Version 9.17.44
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 9.17.45 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 Sixteen(16) signatures to address Thirteen(13) vulnerabilities.

New signatures are added for the following vulnerabilities:

Name	CVE–ID	Category	Severity
OS-WINDOWS Windows Netlogon Elevation of Privilege Vulnerability		Operating System and Services	5
SERVER-OTHER CA ARCserve Backup for Laptops and Desktops LGServer Handshake Buffer Overflow	CVE-2008-3175	Other Web Server	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 Data Protector CRS Opcode 1091 Stack Buffer Overflow	CVE-2013-2334	Other Web Server	1
SERVER-OTHER HP Data Protector CRS Opcode 215 and 263 Stack Buffer Overflow	CVE-2013-2328	Other Web Server	1
SERVER-OTHER HP OpenView Network Node Manager OpenView5 CGI Buffer Overflow	CVE-2008-0067	Other Web Server	1
SERVER-OTHER HP OpenView Network	CVE-2009-4179	Other Web Server	1

Node Manager ovalarm.exe Accept-Language Buffer Overflow			
SERVER-OTHER HP OpenView Network Node Manager ovwebsnmpsrv.exe OVwSelection Buffer Overflow	CVE-2009-4181	Other Web Server	1
SERVER-OTHER HP Operations Agent Performance Component Last Chunk Buffer Overflow	CVE-2012-2019	Other Web Server	1
SERVER-OTHER IBM Tivoli Storage Manager FastBack buffer overflow attempt	CVE-2015-1896	Other Web Server	1
SERVER-WEBAPP Cisco Data Center Network Manager XML external entity injection attempt	CVE-2019-15983	Web Services and Applications	1
SERVER-WEBAPP Microsoft Remote Desktop Connection Manager CVE-2020-0765 XML External Entity Injection	CVE-2020-0765	Web Services and Applications	3

- **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