

SOPHOS

Security made simple.



SOPHOS

IPS Signature Update

Release Notes

Version : 9.17.93

Release Date : 04th March 2021

Release Information

Upgrade Applicable on

IPS Signature Release	Version 9.17.92
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 9.17.93 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 Ten(10) signatures to address Five(5) vulnerabilities.

New signatures are added for the following vulnerabilities:

Name	CVE-ID	Category	Severity
SERVER-OTHER Microsoft Exchange Server CVE-2021-26855 Remote Code ExecutionVulnerability	CVE-2021- 26855	server-other	5
SERVER-OTHER Microsoft Exchange Server Unified Messaging arbitrary codeexecution attempt	CVE-2021- 26857	server-other	1
SERVER-WEBAPP Microsoft Exchange Server arbitrary file writeattempt	CVE-2021- 26858	server- webapp	1
SERVER-WEBAPP Microsoft Exchange Server server side request forgeryattempt	CVE-2021- 26855	server- webapp	1
SERVER-WEBAPP Microsoft Exchange Server server side request forgeryattempt	CVE-2021- 26855	server- webapp	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

©1997 - 2021 Sophos Ltd. All rights reserved.

All rights reserved. Sophos, Sophos logo are trademark of Sophos Technologies Pvt. Ltd.

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