SOPHOS
Security made simple.

SOPHOS
IPS Signature Update
Release Notes

Version : 7.17.93
Release Date : 04th March 2021

Release Information

Upgrade Applicable on

IPS Signature Release	Version 7.17.92
Sophos Appliance Models	XG-550, XG-750, XG-650

Upgrade Information

Upgrade type: Automatic

Compatibility Annotations: None

Introduction

The Release Note document for IPS Signature Database Version 7.17.93 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 Forty Two(42) signatures to address Thirty Two(32) vulnerabilities.

New signatures are added for the following vulnerabilities:

Name	CVE–ID	Category	Severity
BROWSER-WEBKIT TRUFFLEHUNTER TALOS-2021-1238 attackattempt	CVE-2021-21779	browser-webkit	1
FILE-EXECUTABLE TRUFFLEHUNTER TALOS-2021-1255 AttackAttempt	CVE-2021-21785	file-executable	3
FILE-EXECUTABLE TRUFFLEHUNTER TALOS-2021-1255 attackattempt	CVE-2021-21785	file-executable	1
FILE-IMAGE TRUFFLEHUNTER TALOS-2021-1244 Attack Attempt	CVE-2021-21782	file-image	2
FILE-IMAGE TRUFFLEHUNTER TALOS-2021-1244 attackattempt	CVE-2021-21782	file-image	1
FILE-IMAGE TRUFFLEHUNTER TALOS-2021-1248 attack attempt	CVE-2021-21784	file-image	1
FILE-OTHER TRUFFLEHUNTER TALOS-2021-1230 attack attempt		file-other	1
FILE-OTHER TRUFFLEHUNTER		file-other	1

TALOS-2021-1231 attack attempt			
MALWARE-CNC Detected DNSCAT2 C&C Communication		malware-cnc	1
MALWARE-CNC Generic Signature to detect PoshC2 Encrypted C2 Communication		malware-cnc	1
MALWARE-CNC PoshC2 Lateral Movement Attempt Detected		malware-cnc	1
MALWARE-CNC Powershell Empire C2 Traffic Detected		malware-cnc	5
MALWARE-CNC powershellempire C2 Traffic Detected		malware-cnc	1
NETBIOS TRUFFLEHUNTER TALOS-2021-1246 attack attempt		netbios	3
OS-OTHER TRUFFLEHUNTER TALOS-2021-1247 attack attempt		os-other	1
OS-OTHER TRUFFLEHUNTER TALOS-2021-1249 attack attempt		os-other	1
OS-OTHER TRUFFLEHUNTER TALOS-2021-1250		os-other	1

attack attempt			
PROTOCOL-VOIP MultiTech MultiVOIP INVITE Remote CVE-2005-4050 Buffer OverflowVulnerability	CVE-2005-4050	protocol-voip	2
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 D-Link Devices CVE-2019-20215 Unauthenticated Remote CommandExecution In Ssdpcgi	CVE-2019-20215	server-webapp	1
SERVER-WEBAPP Joomla Core Featured Article CVE-2020-10243 SQL InjectionAttempt	CVE-2020-10243	server-webapp	2
SERVER-WEBAPP Microsoft Dynamics365 Finance And Operations CVE-2020-17152Remote Code Execution Attempt	CVE-2020-17152	server-webapp	2
SERVER-WEBAPP Microsoft Exchange Server arbitrary file	CVE-2021-26858	server-webapp	1

writeattempt			
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
SERVER-WEBAPP Microsoft SQL Server 2000 sp_MScopyscript CVE-2002-0645 SQLInjection Vulnerability	CVE-2002-0645	server-webapp	2
SERVER-WEBAPP PHPNuke Remote Arbitrary CVE-2002-0206 File IncludeVulnerability	CVE-2002-0206	server-webapp	2
SERVER-WEBAPP QNAP QTS and Photo Station CVE-2019-7192 Directory TraversalAttempt	CVE-2019-7192	server-webapp	1
SERVER-WEBAPP Ruby on Rails Dynamic Render File Upload CVE-2016-0752 RemoteCode Execution	CVE-2016-0752	server-webapp	3
SERVER-WEBAPP Sun ONE/iPlanet Web Server HTTP TRACE Credential CVE-2003-1567Theft Vulnerability	CVE-2003-1567	server-webapp	2

SERVER-WEBAPP WordPress Comments CVE-2015-3440 Stored Cross SiteScripting	CVE-2015-3440	server-webapp	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