SOPHOS
Security made simple.

SOPHOS
IPS Signature Update
Release Notes

Version : 7.19.51
Release Date : 02nd August 2022

Release Information

Upgrade Applicable on

IPS Signature Release	Version 7.19.50
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 7.19.51 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
BROWSER-WEBKIT Apple Safari WebKit loadInSameDocument use-after-free Attempt	CVE-2022-22620	browser-webkit	2
FILE-IMAGE libpng png_decompress_chunk CVE-2011-3026 Integer Overflow	CVE-2011-3026	file-image	1
FILE-OTHER WECON LeviStudioU Disc Tag WordAddr Stack Buffer Overflow		file-other	2
SERVER-APACHE Apache HTTP Server CVE-2022-31813 Authentication Bypass Vulnerability	CVE-2022-31813	server-apache	1
SERVER-OTHER Delta Industrial Automation DIAEnergie AM_Handler tp SQL Injection		server-other	2
SERVER-OTHER Ivanti Avalanche SmartDeviceServer DeviceLogsManager Directory Traversal		server-other	2
SERVER-WEBAPP Advantech iView getAllActiveTraps search_date CVE-2022-2135 SQL Injection	CVE-2022-2135	server-webapp	1

SERVER-WEBAPP Festo CECC-X-M1 cecc-x-acknerr-request CVE-2022-30310 Command Injection Attempt	CVE-2022-30310	server-webapp	2
SERVER-WEBAPP Festo CECC-X-M1 cecc-x-refresh-request CVE-2022-30311 Command Injection Attempt	CVE-2022-30311	server-webapp	2
SERVER-WEBAPP Festo CECC-X-M1 cecc-x-web-viewer-request CVE-2022-30309 Command Injection Attempt	CVE-2022-30308	server-webapp	2
SERVER-WEBAPP GLPI-Project GLPI Auth.php CVE-2022-31061 SQL Injection Attempt	CVE-2022-31061	server-webapp	1
SERVER-WEBAPP ManageEngine ADAudit Plus cewolf Unauthenticated CVE-2022-28219 Remote Code Execution	CVE-2022-28219	server-webapp	1
SERVER-WEBAPP Roxy-WI CVE-2022-31137 Remote Command Execution	CVE-2022-31137	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	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