SOPHOS
Security made simple.

SOPHOS
IPS Signature Update
Release Notes

Version : 7.19.66
Release Date : 27th September 2022

Release Information

Upgrade Applicable on

IPS Signature Release	Version 7.19.65
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 7.19.66 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 Fourteen(14) signatures to address Ten(10) vulnerabilities.

New signatures are added for the following vulnerabilities:

Name	CVE–ID	Category	Severity
SERVER-WEBAPP Advantech iView findTaskMgrItems sort CVE-2022-2135 SQL Injection	CVE-2022-2135	server-webapp	2
SERVER-WEBAPP Advantech iView NetworkServlet backupDatabase backup_filename CVE-2022-2143 Command Injection	CVE-2022-2143	server-webapp	1
MALWARE-CNC Win.Trojan.Upatre Malware Communication Detected		malware-cnc	1
BROWSER-CHROME Google Chrome V8 CVE-2022-1364 Type Confusion	CVE-2022-1364	browser-chrome	2
BROWSER-CHROME Google Chrome V8 CVE-2021-38003 Heap Corruption	CVE-2021-38003	browser-chrome	2
SERVER-WEBAPP Delta Industrial Automation DIAEnergie Handler_TCV.ashx CVE-2022-1367 SQL Injection	CVE-2022-1367	server-webapp	2
OS-WINDOWS	CVE-2022-	os-windows	1

Microsoft Outlook outlmime.dll Content Type CVE-2022-35742 Denial of Service	35742		
SERVER-WEBAPP OpenEMR fee_sheet_options_ajax .php CVE-2022-2733 Reflected Cross-Site Scripting	CVE-2022-2733	server-webapp	2
MALWARE-OTHER SMBExec- Remote Command Execution Detected SMBv2		malware-other	1
SERVER-WEBAPP Grafana Labs Grafana Unified Alerting CVE-2022-31097 Stored Cross-Site Scripting	CVE-2022-31097	server-webapp	2

- **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