SOPHOS
Security made simple.

SOPHOS
IPS Signature Update
Release Notes

Version : 18.20.29
Release Date : 30th March 2023

Release Information

Upgrade Applicable on

IPS Signature Release	Version 18.20.28
Sophos Appliance Models	XGS Series: XGS 5500, XGS 6500, XGS 7500, XGS 8500 XG Series: XG 550, XG 650, XG 750 SFOS running with RAM >= 24GB on Cloud (AWS, Azure, Nutanix), Virtual Machines and Software appliance

Upgrade Information

Upgrade type: Automatic

Compatibility Annotations: None

Introduction

The Release Note document for IPS Signature Database Version 18.20.29 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 Twenty Two(22) signatures to address Fifteen(15) vulnerabilities.

New signatures are added for the following vulnerabilities:

Name	CVE–ID	Category	Severity
FILE-OFFICE Microsoft Office Outlook appointment privilege escalation attempt	CVE-2023-23397	file-office	1
FILE-OFFICE TRUFFLEHUNTER TALOS-2023-1730 attack attempt		file-office	1
FILE-OTHER GNU Tar from_header CVE-2022-48303 Out-Of-Bounds Read Information Disclosure	CVE-2022-48303	file-other	2
SERVER-OTHER Gogs File Upload tree_path CVE-2022-2024 Command Injection	CVE-2022-2024	server-other	3
SERVER-WEBAPP Cisco IP Phone web interface command injection attempt	CVE-2023-20078	server-webapp	1
SERVER-WEBAPP Cisco IP Phone web interface stack buffer overflow attempt	CVE-2023-20079	server-webapp	1
SERVER-WEBAPP Cisco RV Series Routers CVE-2021-1318 Command Injection Attempt	CVE-2021-1318	server-webapp	3

SERVER-WEBAPP FLIR AX8 Unauthenticated CVE-2022-37061 Remote Code Execution	CVE-2022-37061	server-webapp	1
SERVER-WEBAPP Grandstream GXV31XX Unauthenticated CVE-2019-10655 Command Injection Attempt	CVE-2019-10655	server-webapp	1
SERVER-WEBAPP IBM Aspera Faspex YAML Deserialization CVE-2022-47986 Command Injection Attempt	CVE-2022-47986	server-webapp	1
SERVER-WEBAPP Microsoft Sharepoint CVE-2014-1754 Cross Site Scripting Attempt	CVE-2014-1754	server-webapp	2
SERVER-WEBAPP Microsoft Windows Contacts fnSummaryProc CVE-2022-44666 Remote Code Execution		server-webapp	2
SERVER-WEBAPP Spring Security OAuth2 CVE-2016-4977 Remote Command Execution Vulnerability	CVE-2016-4977	server-webapp	2
SERVER-WEBAPP Zabbix "latest.php" - SQL injection vulnerability CVE-2016-10134 Scanner	CVE-2016-10134	server-webapp	2
SERVER-WEBAPP Zoho	CVE-2022-	server-webapp	1

ManageEngine Multiple Products SAMLResponse Remote Code Execution	47966		

- **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