SOPHOS
Security made simple.

# SOPHOS
# IPS Signature Update
# Release Notes

Version : 18.21.16
Release Date : 21st November 2023

### Release Information

Upgrade Applicable on

| | |
|---|---|
| **IPS Signature Release** | Version 18.21.15 |
| **Sophos Appliance Models** | XGS Series: XGS 5500, XGS 6500, XGS 7500, XGS 8500<br>XG Series: XG 550, XG 650, XG 750<br>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 18.21.16 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(20) signatures to address Fifteen(15) vulnerabilities.

New signatures are added for the following vulnerabilities:

| Name | CVE–ID | Category | Severity |
|---|---|---|---|
| BROWSER-CHROME Google Chrome Origin Trials CVE-2023-2724 Type Confusion Attempt | CVE-2023-2724 | browser-chrome | 2 |
| BROWSER-CHROME Google Chrome Turbofan CVE-2023-4352 Memory Corruption Attempt | CVE-2023-4352 | browser-chrome | 2 |
| BROWSER-OTHER Google Chrome OnItemRemoved CVE-2022-2853 Heap Overflow Attempt | CVE-2022-2853 | browser-other | 2 |
| BROWSER-WEBKIT Apple iOS Webkit CVE-2016-4657 Memory Corruption Vulnerability | CVE-2016-4657 | browser-webkit | 2 |
| FILE-OTHER VISAM VBASE Automation Base ProjektInfo File Parsing CVE-2022-45876 External Entity Injection | CVE-2022-45876 | file-other | 3 |
| FILE-OTHER VISAM VBASE Automation Base ProjektInfo File Parsing CVE-2022-45876 External Entity Injection | CVE-2022-45876 | file-other | 5 |
| OS-LINUX Linux Kernel ksmbd SMB2_QUERY_INFO | CVE-2023-32248 | os-linux | 2 |

| | | | |
|---|---|---|---|
| Handling CVE-2023-32248 NULL Pointer Dereference | | | |
| OS-WINDOWS Microsoft Windows Internet Connection Sharing service remote code execution attempt | CVE-2023-38148 | os-windows | 1 |
| OS-WINDOWS Microsoft Windows Theme code execution attempt | CVE-2023-38146 | os-windows | 2 |
| PROTOCOL-OTHER HTTP/2 rapid reset denial of service attempt | CVE-2023-44487 | protocol-other | 1 |
| SERVER-WEBAPP Cacti Group Cacti sql_save CVE-2023-39357 SQL Injection | CVE-2023-39357 | server-webapp | 2 |
| SERVER-WEBAPP Ivanti Sentry MICSLogService CVE-2023-38035 Command Execution Attempt | CVE-2023-38035 | server-webapp | 1 |
| SERVER-WEBAPP Netgear ProSAFE NMS300 MFileUploadController CVE-2023-38095 Arbitrary File Upload | CVE-2023-38095 | server-webapp | 2 |
| SERVER-WEBAPP XWiki.org Change Request Extension CVE-2023-45138 Code | CVE-2023-45138 | server-webapp | 2 |

| | | | |
|---|---|---|---|
| Injection | | | |
| SERVER-WEBAPP XWiki.org XWiki User Profile CVE-2023-40176 Stored Cross-Site Scripting | CVE-2023-40176 | 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 | 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