SOPHOS
Security made simple.

SOPHOS
IPS Signature Update
Release Notes

Version : 18.21.98
Release Date : 10th June 2024

Release Information

Upgrade Applicable on

IPS Signature Release	Version 18.21.97
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 18.21.98 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 Eleven(11) signatures to address Eleven(11) vulnerabilities.

New signatures are added for the following vulnerabilities:

Name	CVE–ID	Category	Severity
FILE-OTHER TRUFFLEHUNTER TALOS-2024-1993 attack attempt	CVE-2024-26020	file-other	1
POLICY-OTHER Progress OpenEdge potential authentication bypass attempt	CVE-2024-1403	policy-other	1
SERVER-OTHER Delta Industrial Automation DIAEnergie Handler_CFG.ashx CVE-2024-28891 SQL Injection	CVE-2024-28891	server-other	1
SERVER-WEBAPP Adobe ColdFusion CVE-2023-29300 Pre-Authentication Remote Code Execution Vulnerability	CVE-2023-29300	server-webapp	1
SERVER-WEBAPP Check Point Security Gateways CVE-2024-24919 Arbitrary File Read Vulnerability		server-webapp	1
SERVER-WEBAPP F5 BIG-IP Next Central Manager validateUserInCM OData CVE-2024-21793 SQL Injection	CVE-2024-21793	server-webapp	1

SERVER-WEBAPP Fluent Bit CVE-2024-4323 Remote Code Execution Vulnerability		server-webapp	1
SERVER-WEBAPP LG LED Assistant remove3DLUT Directory Traversal		server-webapp	2
SERVER-WEBAPP OpenMetadata Events Subscriptions Validation API CVE-2024-28254 SpEL Injection	CVE-2024-28254	server-webapp	1
SERVER-WEBAPP Schlix CMS v2.2.8-1 CVE-2023-31505 Remote Code Execution	CVE-2023-31505	server-webapp	2
SERVER-WEBAPP WordPress Forminator Plugin SQL Injection	CVE-2024-31077	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