SOPHOS
Security made simple.

SOPHOS
IPS Signature Update
Release Notes

Version : 18.20.16
Release Date : 16th February 2023

Release Information

Upgrade Applicable on

IPS Signature Release	Version 18.20.15
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 18.20.16 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 Nineteen(19) signatures to address Twelve(12) vulnerabilities.

New signatures are added for the following vulnerabilities:

Name	CVE–ID	Category	Severity
MALWARE-CNC Win.Trojan.Azorult outbound connection		malware-cnc	1
MALWARE-CNC Win.Trojan.Ursnif variant outbound connection attempt		malware-cnc	1
MALWARE-CNC Win.Trojan.Ursnif variant outbound connection		malware-cnc	1
OS-WINDOWS Microsoft Malware Protection Engine CVE-2017-0290 Type Confusion Attempt	CVE-2017-0290	os-windows	2
OS-WINDOWS Microsoft Windows NEGOEX CVE-2022-37958 Buffer Overflow	CVE-2022-37958	os-windows	1
PROTOCOL-SCADA Schneider Electric IGSS IGSSdataServer.exe CVE-2022-32525 Opcode 6 Out-Of-Bounds Write	CVE-2022-32525	protocol-scada	2
SERVER-MYSQL Oracle MySQL Cluster Data Node GSN_SYNC_PATH_REQ CVE-2022-21550	CVE-2022-21550	server-mysql	1

Parsing Integer Underflow			
SERVER-MYSQL Oracle MySQL Cluster Data Node GSN_SYNC_PATH_REQ CVE-2022-21550 Parsing Integer Underflow	CVE-2022-21550	server-mysql	5
SERVER-WEBAPP Delta Industrial Automation DIAEnergie InsertReg CVE-2022-41702 Stored Cross-Site Scripting	CVE-2022-41702	server-webapp	3
SERVER-WEBAPP Microsoft SharePoint Workflow IsGoodWorkflowCore CVE-2022-44690 Insecure Deserialization	CVE-2022-44690	server-webapp	3
SERVER-WEBAPP Netgate pfSense pfBlockerNG Host CVE-2022-40624 Command Injection	CVE-2022-40624	server-webapp	1
SERVER-WEBAPP VMware vCenter Server SsoOverRestVerifierUtil CVE-2022-31698 Denial of Service (Decrypted Traffic)		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