SOPHOS
Security made simple.

# SOPHOS
# IPS Signature Update
# Release Notes

Version : 9.16.27
Release Date : 12th September 2019

### Release Information

Upgrade Applicable on

| | |
|---|---|
| **IPS Signature Release** | Version 9.16.26 |
| **Sophos Appliance Models** | CR250i, CR300i, CR500i-4P, CR500i-6P, CR500i-8P, CR500ia, CR500ia-RP, CR500ia1F, CR500ia10F, CR750ia, CR750ia1F, CR750ia10F, CR1000i-11P, CR1000i-12P, CR1000ia, CR1000ia10F, CR1500i-11P, CR1500i-12P, CR1500ia, CR1500ia10F<br>CR25iNG, CR25iNG-6P, CR35iNG, CR50iNG, CR100iNG, CR200iNG/XP, CR300iNG/XP, CR500iNG-XP, CR750iNG-XP, CR2500iNG, CR25wiNG, CR25wiNG-6P, CR35wiNG, CRiV1C, CRiV2C, CRiV4C, CRiV8C, CRiV12C, XG85 to XG450, SG105 to SG650 |

### Upgrade Information

Upgrade type: Automatic

**Compatibility Annotations:** None

## Introduction

The Release Note document for IPS Signature Database Version 9.16.27 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 Sixty Seven(67 ) signatures to address Fifty Four(54) vulnerabilities.

New signatures are added for the following vulnerabilities:

| Name | CVE–ID | Category | Severity |
|---|---|---|---|
| BROWSER-IE Microsoft Internet Explorer VBScript remote code execution attempt | CVE-2018-8174 | Browsers | 2 |
| FILE-FLASH Adobe Flash Player determinePreferredLocales memory corruption attempt | CVE-2017-3114 | Multimedia | 2 |
| FILE-FLASH Adobe Flash Player MP4 atom parser memory corruption attempt | CVE-2017-11281 | Multimedia | 1 |
| FILE-FLASH Adobe Flash Player out of bounds write attempt | CVE-2018-5002 | Multimedia | 2 |
| FILE-FLASH Adobe Flash Player Primetime SDK use after free attempt | CVE-2017-11215 | Multimedia | 1 |
| FILE-IMAGE Adobe Acrobat out-of-bounds write attempt | CVE-2019-7118 | Application and Software | 2 |
| FILE-IMAGE Adobe Acrobat Pro malformed TIFF memory corruption attempt | CVE-2017-11255 | Multimedia | 3 |
| FILE-OTHER Adobe Acrobat CVE-2019-7040 use after free attempt | CVE-2019-7040 | Application and Software | 2 |

| | | | |
|---|---|---|---|
| FILE-OTHER Adobe Acrobat Reader CVE-2018-12791 Use After Free | CVE-2018-12791 | Application and Software | 2 |
| FILE-OTHER Adobe Acrobat type confusion attempt | CVE-2019-7128 | Application and Software | 2 |
| FILE-OTHER EP-IPS ICMP Test Passed | | Application and Software | 5 |
| FILE-OTHER EP-IPS TCP Test Passed | | Application and Software | 5 |
| FILE-OTHER EP-IPS UDP Test Passed | | Application and Software | 5 |
| FILE-PDF Acrobat Reader CVE-2018-12754 Information Disclosure Vulnerability | CVE-2018-12754 | Application and Software | 2 |
| FILE-PDF Acrobat Reader CVE-2018-12758 Information Disclosure Vulnerability | CVE-2018-12758 | Application and Software | 1 |
| FILE-PDF Acrobat Reader CVE-2018-12760 Information Disclosure Vulnerability | CVE-2018-12760 | Application and Software | 2 |
| FILE-PDF Acrobat Reader CVE-2018-5064 Information Disclosure Vulnerability | CVE-2018-5064 | Application and Software | 1 |
| FILE-PDF Acrobat Reader CVE-2018-5070 Information Disclosure Vulnerability | CVE-2018-5070 | Application and Software | 1 |

| | | | |
|---|---|---|---|
| FILE-PDF Adobe Acrobat CVE-2019-7019 out-of-bounds write attempt | CVE-2019-7019 | Application and Software | 2 |
| FILE-PDF Adobe Acrobat CVE-2019-7046 untrusted pointer dereference attempt | CVE-2019-7046 | Application and Software | 2 |
| FILE-PDF Adobe Acrobat CVE-2019-7052 out-of-bounds write attempt | CVE-2019-7052 | Application and Software | 2 |
| FILE-PDF Adobe Acrobat CVE-2019-7118 out-of-bounds write attempt | CVE-2019-7118 | Application and Software | 2 |
| FILE-PDF Adobe Acrobat CVE-2019-7124 out-of-bounds write attempt | CVE-2019-7124 | Application and Software | 2 |
| FILE-PDF Adobe Acrobat PDF Reader CVE-2018-4983 Use After Free | CVE-2018-4983 | Application and Software | 2 |
| FILE-PDF Adobe Acrobat Pro out of bounds write attempt | CVE-2019-7039 | Application and Software | 2 |
| FILE-PDF Adobe Acrobat Reader CVE-2018-4947 Heap Overflow Attempt | CVE-2018-4947 | Application and Software | 2 |
| FILE-PDF Adobe Acrobat Reader CVE-2018-4950 Overflow Attempt | CVE-2018-4950 | Application and Software | 2 |
| FILE-PDF Adobe Acrobat Reader CVE-2018-4969 Overflow Attempt | CVE-2018-4969 | Application and Software | 2 |

| | | | |
|---|---|---|---|
| FILE-PDF Adobe Acrobat Reader CVE-2018-4989 3D Annotations Use After Free | CVE-2018-4989 | Application and Software | 2 |
| FILE-PDF Adobe Acrobat Reader CVE-2019-7119 GIF Memory Corruption | CVE-2019-7119 | Application and Software | 2 |
| FILE-PDF Adobe Acrobat Reader pointer dereference attempt | CVE-2018-4987 | Application and Software | 1 |
| FILE-PDF Adobe Reader CVE-2018-12808 Remote Code Execution Corruption | CVE-2018-12808 | Application and Software | 2 |
| FILE-PDF Adobe Reader CVE-2018-16036 Use After Free | CVE-2018-16036 | Application and Software | 2 |
| FILE-PDF Adobe Reader CVE-2019-7762 Use After Free | CVE-2019-7762 | Application and Software | 2 |
| FILE-PDF Adobe Reader CVE-2019-7765 Use After Free | CVE-2019-7765 | Application and Software | 2 |
| FILE-PDF Adobe Reader CVE-2019-7808 Use After Free | CVE-2019-7808 | Application and Software | 2 |
| FILE-PDF Adobe Reader JavaScript CVE-2018-4961 API Use After Free | CVE-2018-4961 | Application and Software | 2 |
| FILE-PDF Adobe Reader JavaScript resolveNode use-after-free attempt | CVE-2018-19707 | Application and Software | 2 |

| | | | |
|---|---|---|---|
| FILE-PDF Adobe Reader JavaScript resolveNode use-after-free attempt | CVE-2018-19715 | Application and Software | 2 |
| OS-WINDOWS Microsoft SharePoint Insecure De-serialization Vulnerability | CVE-2019-1257 | Operating System and Services | 1 |
| OS-WINDOWS Microsoft SharePoint Insecure De-serialization Vulnerability | CVE-2019-1296 | Operating System and Services | 1 |
| OS-WINDOWS Microsoft Windows DHCP Client CVE-2019-0726 Code Execution | CVE-2019-0726 | Operating System and Services | 1 |
| OS-WINDOWS Microsoft Windows DHCP Client CVE-2019-0726 Code Execution | CVE-2019-0726 | Operating System and Services | 2 |
| OS-WINDOWS Microsoft Windows Kernal Stack Leak Vulnerability | CVE-2019-0788 | Operating System and Services | 1 |
| OS-WINDOWS Microsoft Windows Kernal Stack Leak Vulnerability | CVE-2019-1214 | Operating System and Services | 1 |
| OS-WINDOWS Microsoft Windows Kernal Stack Leak Vulnerability | CVE-2019-1215 | Operating System and Services | 1 |
| OS-WINDOWS | CVE-2019- | Operating | 1 |

| | | | |
|---|---|---|---|
| Microsoft Windows Kernal Stack Leak Vulnerability | 1256 | System and Services | |
| OS-WINDOWS Microsoft Windows Kernal Stack Leak Vulnerability | CVE-2019-1284 | Operating System and Services | 1 |
| OS-WINDOWS Microsoft Windows Remote Desktop Services CVE-2019-1182 Remote Code Execution Vulnerability | CVE-2019-1182 | Operating System and Services | 1 |
| PROTOCOL-DNS Oracle Secure Backup observice.exe dns response overflow attempt | CVE-2010-0072 | DNS | 1 |
| SERVER-APACHE Apache Solr xmlparser XML External Entity Expansion Remote Code Execution | CVE-2017-12629 | Apache HTTP Server | 2 |
| SERVER-ORACLE Oracle WebLogic Server CVE-2018-2894 Web Service Config Arbitrary File Upload | CVE-2018-2894 | Database Management System | 3 |
| SERVER-OTHER HP Intelligent Management Center dbman CVE-2017-5820 BackupZipFile opcode command injection Vulnerability | CVE-2017-5820 | Other Web Server | 1 |

| | | | |
|---|---|---|---|
| SERVER-WEBAPP Oracle WebLogic Server arbitrary JSP file upload attempt | CVE-2018-2894 | Web Services and Applications | 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 | Low |
| 2 | Moderate |
| 3 | High |
| 4 | Critical |

### 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.

Reg. Office: Sophos House, Saigulshan Complex,

Beside White House, Panchvati Cross Road,

Ahmedabad – 380006, INDIA

Phone: +91-79-66216666

Fax: +91-79-26407640

Web site: www.sophos.com