



**SOPHOS**  
**IPS Signature Update**  
**Release Notes**

**Version : 7.16.88**  
**Release Date : 10<sup>th</sup> March 2020**

### Release Information

Upgrade Applicable on

|                         |                        |
|-------------------------|------------------------|
| IPS Signature Release   | Version 7.16.87        |
| Sophos Appliance Models | XG-550, XG-750, XG-650 |

### Upgrade Information

Upgrade type: Automatic

**Compatibility Annotations:** None

### Introduction

The Release Note document for IPS Signature Database Version 7.16.88 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](mailto:support@sophos.com), along with the application details.

This IPS Release includes Five(5) signatures to address Five(5) vulnerabilities.

New signatures are added for the following vulnerabilities:

| Name  | CVE-ID        | Category              | Severity |
|---|---------------|-----------------------|----------|
| BROWSER-IE Internet Explorer Scripting Engine CVE-2020-0833 Memory Corruption Vulnerability | CVE-2020-0833 | Browsers              | 1        |
| BROWSER-IE Internet Explorer VBScript CVE-2020-0847 Remote Code Execution Vulnerability     | CVE-2020-0847 | Browsers              | 1        |
| BROWSER-IE Microsoft Internet Explorer CVE-2020-0824 VBScript Engine Remote Code Execution  | CVE-2020-0824 | Browsers              | 2        |
| BROWSER-IE Microsoft Internet Explorer CVE-2020-0832 Engine Memory Corruption               | CVE-2020-0832 | Browsers              | 2        |
| MALWARE-CNC Blue Coat BCAA Stack Buffer Overflow  |               | Malware Communication | 2        |

- **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**

©1997 - 2020 Sophos Ltd. All rights reserved.

All rights reserved. Sophos, Sophos logo are trademark of Sophos Technologies Pvt. Ltd.

### **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](http://www.sophos.com)