

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tp/>

DATE(S) ISSUED:

04/01/2015

SUBJECT:

Multiple Vulnerabilities in Websense TRITON V-Series

OVERVIEW:

Multiple vulnerabilities have been discovered in Websense TRITON V-Series software, which could allow an attacker to take complete control of an affected system. Websense TRITON V-Series are appliances that are based on a preconfigured, security-hardened platform designed to support flexible deployment of security solutions.

The exploitation of these vulnerabilities could allow for remote code execution on the device or may cause denial of service conditions.

THREAT INTELLIGENCE:

There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEM AFFECTED:

Websense TRITON V-Series prior to 8.0.0

RISK:

Government:

Large and medium government entities: **High**

Small government entities: **High**

Businesses:

Large and medium business entities: **High**

Small business entities: **High**

Home users: N/A

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Websense TRITON V-Series that may result in remote code execution. They are as follows:

- Cross-Site Request Forgery (CSRF) in command line page (CVE 2015-2770) - A vulnerability in the command line page in Websense TRITON V-Series that allows remote attackers to hijack the authentication of unspecified victims.
- Mail Server Accepts Plaintext Credentials QualysGuard Potential Vulnerability (CVE-2015-2771) - A vulnerability in which credentials are received in plaintext which may allow attackers to obtain sensitive information.
- Unspecified Arbitrary File Upload Vulnerability (CVE-2015-2772) - An unspecified file-upload vulnerability that an attacker could leverage to upload arbitrary files to the affected machine resulting in code execution.

- Unspecified Arbitrary File Read Vulnerability (CVE-2015-2773) - An unspecified arbitrary file read vulnerability that could allow an attacker to read arbitrary files in the context of the user running the application.

RECOMMENDATIONS:

The following actions should be taken:

Apply appropriate patches provided by Websense to vulnerable systems immediately after appropriate testing.

Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

REFERENCES:**Websense:**

<http://www.websense.com/support/article/kbarticle/Vulnerabilities-resolved-in-TRITON-APX-Version-8-0>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2770>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2771>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2772>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2773>

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

<http://www.us-cert.gov/tlp/>