

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/tlp/>

DATE(S) ISSUED:

3/26/2015

SUBJECT:

Multiple Vulnerabilities in Cisco Products

OVERVIEW:

Multiple vulnerabilities have been discovered in several Cisco products, including Cisco IOS, Cisco IOS XE, Cisco ASR 1000 Series, Cisco ISR 4400 Series, and Cisco Cloud Services 1000v Series Routers. These products provide firewall, intrusion prevention, remote access, and other services.

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:

Cisco IOS 15.4(3)SN1 and earlier versions

Cisco IOS XE Software 3.13S .0 and earlier versions

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:

Cisco Products are prone to multiple vulnerabilities that could allow for remote code execution or denial of service. These vulnerabilities are as follows:

Cisco IOS Software is prone to multiple vulnerabilities that could allow for denial of service. These vulnerabilities are as follows:

A vulnerability within the virtual routing and forwarding (VRF) subsystem of Cisco IOS software could allow an attacker to cause a denial of service (DoS) condition. (CVE 2015-0638)

Multiple vulnerabilities in how Cisco IOS processes crafted Common Industrial Protocol (CIP) IP version 4 (IPv4) packets that could allow an attacker to cause a denial of service (DoS) condition. (CVE 2015-0647, CVE 2015-0648, CVE 2015-0649)

Cisco IOS and IOS XE are prone to multiple vulnerabilities that could allow for denial of service. These vulnerabilities are as follows:

Multiple vulnerabilities in the Autonomic Networking Infrastructure (ANI) feature that could allow an attacker to spoof an Autonomic Networking Registration Authority (ANRA) response and cause a denial of service (DoS) condition (CVE 2015-0635, CVE 2015-0636, CVE 2015-0637)

Multiple vulnerabilities within the Internet Key Exchange (IKE) version 2 subsystem that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. (CVE 2015-0642, CVE 2015-0643)

A vulnerability in the multicast DNS (mDNS) gateway function of Cisco IOS Software and Cisco IOS XE Software could allow an attacker to reload the vulnerable device. (CVE 2015-0650)

A vulnerability in the TCP input module of Cisco IOS and Cisco IOS XE Software that could allow an attacker to cause a memory leak and eventual reload of the affected device. (CVE 2015-0646)

Cisco IOS XE software for Cisco ASR 1000 Series, Cisco ISR 4400 Series, and Cisco Cloud Services 1000v Series Routers are prone to multiple vulnerabilities that could allow for denial of service or remote code execution. These vulnerabilities are as follows:

A vulnerability in the high-speed logging (HSL) functionality that could allow an attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition (CVE-2015-0640)

A vulnerability in the AppNav component that could allow an unauthenticated, remote attacker to cause an affected device to reload and may allow arbitrary code execution on the affected system. (CVE-2015-0644)

A vulnerability in IP version 6 (IPv6) parsing that could allow an attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. (CVE-2015-0641)

A vulnerability in the Layer 4 Redirect (L4R) processing code that could allow an attacker to cause a reload of the affected device. (CVE-2015-0645)

A vulnerability in the Common Flow Table (CFT) processing that could allow an attacker to cause a reload of the affected device. (CVE-2015-0639)

RECOMMENDATIONS:

The following actions should be taken:

Apply software updates provided by Cisco, and workarounds that mitigate these vulnerabilities are also available from Cisco at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar15.html

REFERENCES:

Cisco:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_mar15.html

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0635>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0636>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0637>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0638>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0639>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0640>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0641>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0642>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0643>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0644>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0645>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0646>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0647>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0648>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0649>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0650>

TLP: WHITE

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

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