

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:

02/10/2016

SUBJECT:

Buffer Overflow Vulnerability in Cisco ASA Software Products Could Allow for Remote Code Execution

OVERVIEW:

A buffer overflow vulnerability has been discovered in Cisco ASA Adaptive Security Appliances. Successful exploitation could allow an unauthenticated user to take control of the affected system and perform unauthorized actions.

THREAT INTELLIGENCE:

This exploit has been publicly disclosed. There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500-X Series Next-Generation Firewalls
- Cisco ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers
- Cisco ASA 1000V Cloud Firewall
- Cisco Adaptive Security Virtual Appliance (ASAv)
- Cisco Firepower 9300 ASA Security Module
- Cisco ISA 3000 Industrial Security Appliance

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 ASA Software IKEv1 and IKEv2 are prone to a buffer overflow vulnerability that could allow for an unauthenticated user to cause a reload of the affected system or to remotely execute code. The algorithm for re-assembling Internet Key Exchange (IKE) payloads fragmented with the Cisco fragmentation protocol contains a bounds-checking flaw that allows a heap buffer to be overflowed with specially crafted UDP packets.

RECOMMENDATIONS:

The following actions should be taken:

- Install updates provided by Cisco immediately after appropriate testing.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Monitor intrusion detection systems for any signs of anomalous activity.
- Unless required, limit external network access to affected products.

REFERENCES:

Cisco:

<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160210-asa-ike>

Exodus:

<https://blog.exodusintel.com/2016/01/26/firewall-hacking/>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1287>

TLP: WHITE

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

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