

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.

DATE(S) ISSUED:

04/10/2014

SUBJECT:

Multiple Vulnerabilities in Cisco ASA Software

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been discovered in Cisco Adaptive Security Appliance (ASA) Software which is the operating system used by Cisco ASA appliances. The exploitation of these vulnerabilities could allow a remote attacker to gain unauthorized access to the internal network via SSL VPN, or to elevate privileges and gain administrative access to the affected system, or even cause the exhaustion of available memory which may cause denial of service conditions.

THREAT INTELLIGENCE

Currently we are not aware of any malicious exploitation of these vulnerabilities in the wild.

SYSTEMS AFFECTED:

Cisco ASA software running on the following Cisco products is affected by these vulnerabilities:

- 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 Routers
- Cisco ASA 1000V Cloud Firewall

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: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in Cisco ASA Software which is the operating system used by Cisco ASA appliances. The affected appliances provide network security services such as firewall, intrusion prevention, and VPN. It should be noted that these vulnerabilities are independent of one another. In other words, a Cisco ASA system that is affected by one of these vulnerabilities may not be affected by the others. Please see the following link to Cisco's advisory and find the sub-menu for "Software Versions and Fixes" to find a detailed graph describing which versions of the Cisco ASA Software is affected by which vulnerability:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-asa>

Cisco ASA SSL VPN Authentication Bypass Vulnerability

A vulnerability in the SSL VPN code could allow an unauthenticated remote attacker to access the SSL VPN portal web page. This vulnerability is due to improper handling of authentication cookies when the Cisco ASA SSL VPN feature is enabled. An attacker could exploit this vulnerability by manually modifying the HTTP POST body with a forged cookie value or entering a crafted URL. Depending on the SSL VPN configuration, the attacker may be able to start a VPN tunnel using Cisco AnyConnect. However, in all cases, the attacker may gain unauthorized access to internal network resources.

Cisco ASA SSL VPN Privilege Escalation Vulnerability

A vulnerability in the code that handles management session information could allow an authenticated remote attacker to elevate the assigned privilege and gain administrative access to the affected system. The vulnerability is due to improper validation of user privileges when users are connected to the SSL VPN portal by using the clientless SSL VPN feature. An attacker could exploit this vulnerability by logging in to the SSL VPN portal and submitting crafted URLs.

Cisco ASA ASDM Privilege Escalation Vulnerability

A vulnerability in the code that handles privilege assignment when the Cisco ASA device is accessed using the Cisco Adaptive Security Device Manager (ASDM) could allow an authenticated remote attacker to elevate privileges and gain administrative access to the affected system. The vulnerability is due to improper privilege assignment to users with privilege level 0. An attacker could exploit this vulnerability by logging into the Cisco ASDM with user credentials and a privilege level of 0.

Cisco ASA SIP Denial of Service Vulnerability

A vulnerability in the Session Initiation Protocol (SIP) inspection engine code could allow an unauthenticated remote attacker to exhaust available memory which may cause system instability, or a reload of the affected system. The vulnerability is due to improper handling of SIP packets inspected by the Cisco ASA SIP inspection engine. An attacker can exploit this vulnerability by sending crafted SIP packets through the affected system. Exploiting this vulnerability may create denial of service conditions on the affected system.

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://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-asa>

REFERENCES:

Cisco:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-asa>

Security Focus:

<http://www.securityfocus.com/bid/66745>

<http://www.securityfocus.com/bid/66746>

<http://www.securityfocus.com/bid/66747>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2126>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2128>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2129>