

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:

10/09/2013

SUBJECT:

Multiple Vulnerabilities in Cisco ASA Software Could Allow Remote Access or Denial of Service

OVERVIEW:

Multiple vulnerabilities have been discovered in Cisco Adaptive Security Appliance (ASA) Software running on multiple platforms. Cisco ASA software provides firewall, intrusion prevention, remote access, and other services. Successful exploitation of some of the vulnerabilities could lead to an attacker gaining remote access to the system or network. The remaining vulnerabilities could result in denial of service conditions or instability of the affected device.

SYSTEMS AFFECTED:

- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco ASA 5500-X Next Generation Firewall Appliances
- Cisco Catalyst 6500 Series ASA Services Module
- 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: N/A

DESCRIPTION:

Multiple vulnerabilities have been discovered in Cisco Adaptive Security Appliance (ASA) Software running on multiple platforms. Cisco ASA software provides firewall, intrusion prevention, remote access, and other services. Successful exploitation of some of the

vulnerabilities could lead to an attacker gaining remote access to the system or network. The remaining vulnerabilities could result in denial of service conditions or instability of the affected device.

These vulnerabilities are independent of one other; a release that is affected by one of the vulnerabilities may not be affected by the others.

IPsec VPN Crafted ICMP Packet Denial of Service Vulnerability

A vulnerability in IPsec code could allow an unauthenticated, remote attacker to cause a reload of an affected device.

SQL*Net Inspection Engine Denial of Service Vulnerability

A vulnerability in SQL*Net inspection engine code could allow an unauthenticated, remote attacker to cause a reload of the affected system.

Digital Certificate Authentication Bypass Vulnerability

A vulnerability in the code for SSL certificate validation of the Cisco ASA Software could allow an unauthenticated, remote attacker to bypass the certificate authentication.

Remote Access VPN Authentication Bypass Vulnerability

A vulnerability in the authentication code of the remote access VPN feature of Cisco ASA Software could allow an unauthenticated, remote attacker to bypass the remote VPN authentication, which could allow remote access to the inside network.

Digital Certificate HTTP Authentication Bypass Vulnerability

A vulnerability in the authentication code of remote management via Cisco Adaptive Security Device Management (ASDM) could allow an unauthenticated, remote attacker to bypass the digital certificate authentication. Depending on the configuration, this may allow the attacker to remotely connect as administrator to the management interface via Cisco ASDM and take full control of the affected system.

HTTP Deep Packet Inspection Denial of Service Vulnerability

A vulnerability in HTTP Deep Packet Inspection (DPI) code could allow an unauthenticated, remote attacker to cause a reload of the affected system.

DNS Inspection Denial of Service Vulnerability

A vulnerability in the DNS Application Layer Protocol Inspection (ALPI) engine of Cisco ASA Software could allow an unauthenticated, remote attacker to trigger a reload of the affected device.

AnyConnect SSL VPN Memory Exhaustion Denial of Service Vulnerability

A vulnerability in how Cisco ASA Software handles AnyConnect SSL VPN client

connections could allow an unauthenticated, remote attacker to exhaust available memory which could cause the affected system to become unresponsive and transit traffic to be dropped.

Clientless SSL VPN Denial of Service Vulnerability

A vulnerability in the Clientless SSL VPN code could allow an unauthenticated, remote attacker to cause the reload of the affected system.

RECOMMENDATIONS:

The following actions should be taken:

Upgrade vulnerable Cisco products immediately after appropriate testing.

REFERENCES:

CISCO:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20131009-asa>

<http://tools.cisco.com/security/center/viewAlert.x?alertId=31101>

<http://tools.cisco.com/security/center/viewAlert.x?alertId=31107>

<http://tools.cisco.com/security/center/viewAlert.x?alertId=31105>

<http://tools.cisco.com/security/center/viewAlert.x?alertId=31104>

<http://tools.cisco.com/security/center/viewAlert.x?alertId=31103>

<http://tools.cisco.com/security/center/viewAlert.x?alertId=31106>

<http://tools.cisco.com/security/center/viewAlert.x?alertId=31102>

<http://tools.cisco.com/security/center/viewAlert.x?alertId=31101>

<http://tools.cisco.com/security/center/viewAlert.x?alertId=31098>

<http://tools.cisco.com/security/center/viewAlert.x?alertId=31100>