

*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:**

10/08/2014

**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 6500/7600 Series ASA Services Module
- Cisco ASA 1000V Cloud Firewall
- Cisco Adaptive Security Virtual Appliance (ASAv)

**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.

**Cisco ASA 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.

**Cisco ASA VPN Denial of Service Vulnerability**

A vulnerability in the IKE code of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause the reload of an affected system.

**Cisco ASA IKEv2 Denial of Service Vulnerability**

A vulnerability in the IKEv2 code of Cisco ASA Software could allow an unauthenticated, remote attacker to cause the reload of an affected system.

**Cisco ASA Health and Performance Monitor Denial of Service Vulnerability**

A vulnerability in Health and Performance Monitoring (HPM) for ASDM functionality of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause a reload of an affected device and eventual denial of service (DoS) condition.

**Cisco ASA GPRS Tunneling Protocol Inspection Engine Denial of Service Vulnerability**

A vulnerability in the GPRS Tunneling Protocol (GTP) inspection engine of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause the reload of an affected system.

**Cisco ASA SunRPC Inspection Engine Denial of Service Vulnerability**

A vulnerability in the SunRPC inspection engine of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause the reload of an affected system.

**Cisco ASA DNS Inspection Engine Denial of Service Vulnerability**

A vulnerability in the DNS inspection engine of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause the reload of an affected system.

**Cisco ASA VPN Failover Command Injection Vulnerability**

A vulnerability in the VPN code of Cisco ASA Software could allow an authenticated, remote attacker to submit configuration commands to the standby unit via the failover interface. As result, an attacker could be able to take full control of both the active and standby failover units.

#### **Cisco ASA VNMC Command Input Validation Vulnerability**

A vulnerability in the Virtual Network Management Center (VNMC) policy code of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, local attacker to access the underlying Linux operating system with the privileges of the root user.

#### **Cisco ASA Local Path Inclusion Vulnerability**

A vulnerability in the function that exports environment variables of Cisco ASA Software could allow an authenticated, local attacker to inject a malicious library and take complete control of the system.

#### **Cisco ASA Clientless SSL VPN Information Disclosure and Denial of Service Vulnerability**

A vulnerability in the Clientless SSL VPN portal feature could allow an unauthenticated, remote attacker to access random memory locations. Due to this vulnerability, the attacker may be able to access the information stored in memory and in some cases may be able to corrupt this portion of memory, which could lead to a reload of the affected system.

#### **Cisco ASA Clientless SSL VPN Portal Customization Integrity Vulnerability**

A vulnerability in the Clientless SSL VPN portal customization framework could allow an unauthenticated, remote attacker to modify the content of the Clientless SSL VPN portal, which could lead to several attacks including the stealing of credentials, cross-site scripting (XSS), and other types of web attacks on the client using the affected system.

#### **Cisco ASA Smart Call Home Digital Certificate Validation Vulnerability**

A vulnerability in the Smart Call Home (SCH) feature of Cisco ASA Software could allow an unauthenticated, remote attacker to bypass digital certificate validation if any feature that uses digital certificates is configured on 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-20141008-asa>

<https://tools.cisco.com/bugsearch/bug/CSCum46027>

<https://tools.cisco.com/bugsearch/bug/CSCul36176>

<https://tools.cisco.com/bugsearch/bug/CSCum96401>

<https://tools.cisco.com/bugsearch/bug/CSCum00556>

<https://tools.cisco.com/bugsearch/bug/CSCum56399>

<https://tools.cisco.com/bugsearch/bug/CSCun11074>

<https://tools.cisco.com/bugsearch/bug/CSCuo68327>

<https://tools.cisco.com/bugsearch/bug/CSCuq28582>

<https://tools.cisco.com/bugsearch/bug/CSCuq41510>

<https://tools.cisco.com/bugsearch/bug/CSCtq52661>

<https://tools.cisco.com/bugsearch/bug/CSCuq29136>

<https://tools.cisco.com/bugsearch/bug/CSCup36829>

<https://tools.cisco.com/bugsearch/bug/CSCun10916>