

*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:**

10/26/2015

**SUBJECT:**

Multiple Vulnerabilities in Cisco ASA Software

**OVERVIEW:**

Multiple vulnerabilities have been discovered in Cisco Adaptive Security Appliance (ASA) Software. The Cisco ASA family provides network security services such as firewall, intrusion prevention system (IPS), endpoint security (anti-x), and VPN.

The exploitation of these vulnerabilities could allow for denial of service conditions.

**THREAT INTELLIGENCE**

There are currently no reports of these vulnerabilities being exploited in the wild.

**SYSTEM AFFECTED:**

- Versions 8.2 prior to Cisco Adaptive Security Appliance Software 8.2(5.58)
- Versions 8.3, upgrade to Cisco Adaptive Security Appliance Software 8.4(7.29) or later
- Versions 8.4 prior to Cisco Adaptive Security Appliance Software 8.4(7.29)
- Versions 8.5 and 8.6, upgrade to Cisco Adaptive Security Appliance Software 9.0(4.37) or later
- Versions 8.7 prior to Cisco Adaptive Security Appliance Software 8.7(1.17)
- Versions 9.0 prior to Cisco Adaptive Security Appliance Software 9.0(4.37)
- Versions 9.1 prior to Cisco Adaptive Security Appliance Software 9.1(6.8)
- Versions 9.2 prior to Cisco Adaptive Security Appliance Software 9.2(4)
- Versions 9.3 prior to Cisco Adaptive Security Appliance Software 9.3(3.5)
- Versions 9.3 prior to Cisco Adaptive Security Appliance Software 9.4(2)

**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:**

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

**Cisco ASA Software is prone to the following vulnerabilities:**

- A vulnerability in the Internet Key Exchange (IKE) version 1 (v1) code could allow an unauthenticated, remote attacker to cause an affected system to reload. (CVE-2015-6327)
- A vulnerability in the DNS code could allow an unauthenticated, remote attacker to cause an affected system to reload. (CVE-2015-6325)
- A vulnerability in the DHCPv6 relay feature of could allow an unauthenticated, remote attacker to cause an affected device to reload. (CVE-2015-6324)
- A vulnerability in the DNS code could allow an unauthenticated, remote attacker to cause an affected system to reload. (CVE-2015-6326)
- A vulnerability in the DHCPv6 relay feature could allow an unauthenticated, remote attacker to cause an affected device to reload. (CVE-2015-0578)

**RECOMMENDATIONS:**

The following actions should be taken:

- Apply software updates provided by Cisco, and workarounds that mitigate these vulnerabilities immediately after appropriate testing.

**REFERENCES:**

**Cisco:**

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150115-asa-dhcp>

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-asa-dns2>

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-asa-dhcp1>

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-asa-dns1>

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-asa-ike>

**CVE:**

<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6327>

<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6325>

<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6324>

<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6326>

<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0578>

**Others:**

<https://exchange.xforce.ibmcloud.com/vulnerabilities/100549>

<http://www.securitytracker.com/id/1031542>

**TLP: WHITE**

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

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