



**State of Alaska Cyber Security &  
Critical Infrastructure  
Cyber Advisory**

**April 11, 2013**

*The following cyber advisory was issued by the State of Alaska and was 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.*

**ADVISORY NUMBER:**

SA2013-036

**DATE(S) ISSUED:**

04/11/2013

**SUBJECT:**

Multiple Denial of Service Vulnerabilities in Cisco Products

**OVERVIEW:**

Multiple vulnerabilities have been discovered in several Cisco products, including Cisco Adaptive Security Appliance (ASA) 5500 Series, Cisco Catalyst 6500 Series ASA and Firewall Services Module (FWSM), Cisco 7600 Series Routers ASA and FWSM, Cisco ASA 1000V Cloud Firewall, as well as Cisco 1000 Series Aggregation Services Routers (ASR) running Cisco IOS XE. These products provide firewall, intrusion prevention, remote access, and other services. Successful exploitation of these vulnerabilities could result in denial of service conditions or reboot of the affected device.

**SYSTEMS AFFECTED:**

- **Cisco Adaptive Security Appliance (ASA) Software for:**
  - Cisco ASA 5500 Series Adaptive Security Appliances
  - Cisco ASA Services Module for Cisco Catalyst 6500 Series Switches
  - Cisco ASA Services Module for Cisco 7600 Series Routers
  - Cisco ASA 1000V Cloud Firewall
- **Cisco Firewall Services Module (FWSM) Software for:**
  - Cisco Catalyst 6500 Series Switches
  - Cisco 7600 Series Routers
- **Cisco IOS XE Software for:**
  - Cisco 1000 Series Aggregation Services Routers (ASR)

**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 Cisco products are vulnerable to a remote Denial of Service condition. The details of each vulnerable Cisco product are provided below.

**Cisco Adaptive Security Appliance (ASA) 5500 Series, Cisco Catalyst 6500 Series ASA and Firewall Services Module (FWSM), Cisco 7600 Series Routers ASA and FWSM, Cisco ASA 1000V Cloud Firewall**

To exploit these vulnerabilities, an attacker needs to create a specially crafted packet that will result in denial of service when processed by the device. Affected versions of Cisco ASA and FWSM software will vary depending on the specific vulnerability.

The details of the vulnerabilities are as follows:

- Cisco ASA and Cisco FWSM are prone to a remote denial-of-service vulnerability because they fail to properly process an incoming IKE version 1 message. An attacker can exploit this vulnerability by sending a crafted IKE message, causing a reload of an affected device, denying service to legitimate users. Switching to IKE version 2 will mitigate this vulnerability. This issue is being tracked by Cisco Bug IDs CSCub85692 and CSCud20267 (CVE-2013-1149).
- Cisco FWSM for the Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers is prone to a denial-of-service vulnerability due to the incorrect processing of URLs. Specifically, this issue occurs when clients make requests through the auth-proxy feature. An attacker can exploit this issue to cause a vulnerable device to reload, triggering a denial-of-service condition. Disabling AAA for network access control and HTTP(S) listening ports to authenticate network users, if feasible, will mitigate this vulnerability. This issue is tracked by Cisco Bug ID CSCtg02624 (CVE-2013-1155).
- Cisco Adaptive Security Appliance (ASA) is prone to a remote denial-of-service vulnerability. Specifically, this issue occurs in the URL processing code of the authentication proxy feature. An attacker can exploit this vulnerability by sending a crafted URL, causing a reload of an affected device, denying service to legitimate users. This issue is being tracked by Cisco Bug ID CSCud16590 (CVE-2013-1150).
- Cisco Adaptive Security Appliance (ASA) is prone to a remote denial-of-service vulnerability due to an implementation error in the code that validates the digital certificates used during authentication. An attacker can exploit this issue by using a crafted certificate to trigger an authentication operation on an affected device, causing a reload of an affected device, denying service to legitimate users. This issue is being tracked by Cisco Bug ID CSCuc72408 (CVE-2013-1151)
- Cisco Adaptive Security Appliance (ASA) is prone to a remote denial-of-service vulnerability that occurs in the DNS inspection engine code. Specifically, this issue occurs because of improper processing of certain fields in DNS messages. An attacker can exploit this issue by sending a crafted DNS message, causing a reload of an affected device, denying service to legitimate users. Disabling DNS inspection, if feasible, will

mitigate this vulnerability. This issue is being tracked by Cisco Bug ID CSCuc80080 (CVE-2013-1152).

### **Cisco IOS XE Software for Cisco 1000 Series Aggregation Services Router (ASR).**

To exploit these vulnerabilities, an attacker needs to create a specially crafted packet that will result in denial of service when processed by the software. Affected versions of Cisco IOS XE Software for 1000 Series ASR will vary depending on the specific vulnerability.

The details of the vulnerabilities are as follows:

- Improper handling of fragmented IPv6 multicast and IPv6 MVPN traffic by Cisco 1000 Series ASR with ASR1000-ESP40 or ASR1000-ESP100 may allow an attackers to cause a reload of the affected devices, denying service to legitimate users. This issue is being tracked by Cisco Bug IDs CSCtz97563 and CSCub34945 (CVE-2013-1164).
- Improper handling of specific L2TP packets by Cisco 1000 ASR may allow an attackers to cause a reload of the affected devices, denying service to legitimate users. Repeated attacks will result in a sustained denial of service. This issue is being tracked by Cisco Bug ID CSCtz23293 (CVE-2013-1165).
- Improper handling of packets by Cisco 1000 Series ASR configured for bridge domain interface (BDI) may allow an attackers to cause a reload of the affected devices, denying service to legitimate users. Repeated attacks will result in a sustained denial of service. This issue is being tracked by Cisco Bug ID CSCtt11558 (CVE-2013-1167).
- Improper handling of a large number SIP packets by Cisco 1000 Series ASR when configured for VRF-aware NAT and SIP ALG may allow an attackers to cause a reload of the affected devices, denying service to legitimate users. Repeated attacks will result in a sustained denial of service. This issue is being tracked by Cisco Bug ID CSCuc65609 (CVE-2013-1166).

### **RECOMMENDATIONS:**

We recommend the following actions be taken:

- Upgrade vulnerable Cisco products immediately after appropriate testing.
- Consider migrating from IKE version 1 to IKE version 2.

### **REFERENCES:**

#### **Cisco:**

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130410-asa>

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130410-fwsm>

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20130410-asr1000>

#### **SecurityFocus:**

<http://www.securityfocus.com/bid/59001>

<http://www.securityfocus.com/bid/59002>

<http://www.securityfocus.com/bid/59003>

<http://www.securityfocus.com/bid/59004>

<http://www.securityfocus.com/bid/59005>

<http://www.securityfocus.com/bid/59007>

<http://www.securityfocus.com/bid/59008>

<http://www.securityfocus.com/bid/59009>

<http://www.securityfocus.com/bid/59012>

**CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1149>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1150>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1151>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1152>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1155>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1164>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1165>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1166>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-1167>