



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

**April 9, 2015**

*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:**

SA2015-038

**DATE(S) ISSUED:**

4/09/2015

**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 complete system compromise on the device or may cause denial of service conditions.

**THREAT INTELLIGENCE**

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

**SYSTEM AFFECTED:**

- Versions prior to Cisco Adaptive Security Appliance 9.2(3.3)
- Versions prior to Cisco Adaptive Security Appliance (ASA) Software 9.1(6)
- Versions prior to Cisco Adaptive Security Appliance (ASA) Software 9.3(3)
- Versions prior to Cisco ASA FirePOWER Software 5.3.1.2
- Versions prior to Cisco ASA CX Software 9.3.2.1-9

## 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 complete system compromise or denial of service. These vulnerabilities are as follows:

Cisco ASA Software is prone to the following vulnerabilities:

- A vulnerability in the improper handling of secured failover communication messages when the failover IPsec feature is configured that may allow an unauthenticated, remote attacker to cause a complete system compromise. (CVE 2015-0675)
- A vulnerability in the improper processing of DNS packets that may allow an unauthenticated, remote attacker the ability to cause denial-of-service conditions. (CVE 2015-0676)
- A vulnerability in the insufficient hardening of the XML parser configuration that may allow an unauthenticated, remote attacker the ability to cause denial of service conditions. (CVE 2015-0677)

Cisco ASA FirePOWER Services and Cisco ASA CX Services are prone to the following vulnerability:

- A vulnerability in the improper handling of crafted packets sent at a high rate to the management interface that may allow an unauthenticated, remote attacker the ability to cause denial-of-service conditions. (CVE 2015-0678)

## RECOMMENDATIONS:

We recommend the following actions 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-20150408-asa>

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150408-cxftp>

<http://tools.cisco.com/security/center/viewAlert.x?alertId=38183>

<http://tools.cisco.com/security/center/viewAlert.x?alertId=38184>

<http://tools.cisco.com/security/center/viewAlert.x?alertId=38185>

<http://tools.cisco.com/security/center/viewAlert.x?alertId=38186>

### CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0675>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0676>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0677>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0678>

### Security Focus:

<http://www.securityfocus.com/bid/73966>

<http://www.securityfocus.com/bid/73967>

<http://www.securityfocus.com/bid/73968>

<http://www.securityfocus.com/bid/73969>