



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

March 15, 2012

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:

SA2012-016

DATE(S) ISSUED:

3/15/2012

SUBJECT:

Multiple Vulnerabilities in Cisco ASA 5500 Series Products and Cisco ASA Modules for Catalyst 6500 Switches

OVERVIEW:

Multiple vulnerabilities have been discovered in Cisco Adaptive Security Appliance (ASA) 5500 series appliances and ASA modules for Catalyst 6500 series switches. Cisco ASA products provide firewall, intrusion prevention, remote access, and other services. Successful exploitation could lead to the attacker taking control of a client machine or cause the appliance to reload, creating denial-of-service conditions.

SYSTEMS AFFECTED:

- Cisco ASA 5500 Series Appliances
- Cisco Catalyst 6500 series ASA Service Modules

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 ASA 5500 Series Appliances and Cisco Catalyst 6500 series ASA Service Modules that could result in denial-of-service conditions. Details of these vulnerabilities are as follows:

Cisco ASA 5500 Clientless VPN Remote Code Execution Vulnerability

Cisco ASA 5500 series products distribute an ActiveX control that is prone to a remote code execution vulnerability. The Clientless VPN allows users to connect to an intranet through an SSL tunnel using a web browser. When users connect to the ASA device it distributes and installs an ActiveX control to the client machine; which is used to initiate and maintain the tunnel. This ActiveX control is prone to a buffer overflow vulnerability that could allow for remote code execution on the client machine. To exploit this vulnerability, an attacker locates a machine that has downloaded and installed the vulnerable ActiveX control. The attacker then entices the user to visit a specially crafted website, usually through e-mail. When the site is visited the exploit is triggered. Successful exploitation could result in remote code execution. A workaround are currently available to mitigate this issue. This vulnerability affects software releases 7.0, 7.1, 7.2, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6.(CVE-2012-0358)

Cisco ASA UDP Inspection Engine Denial-of-Service Vulnerability

Cisco ASA 5500 series products and Catalyst 6500 ASA Service Modules are prone to a remote denial-of-service vulnerability when handing specially crafted UDP packets with the inspection engine. The Cisco ASA inspection engine is used as part of a stateful firewall implementation. UDP inspection vulnerabilities exists in the following engines:

- Domain Name System (DNS)
- Session Initiation Protocol (SIP)
- Simple Network Management Protocol (SNMP)
- GPRS Tunneling Protocol (GTP)
- H.323, H.225 RAS
- Media Gateway Control Protocol (MGCP)
- SunRPC
- Trivial File Transfer Protocol (TFTP)
- X Display Manager Control Protocol (XDMCP)
- IBM NetBios
- Instant Messaging (depending on the particular IM client/solution being used)

To exploit these vulnerabilities, an attacker sends specially crafted UDP packets (for the services listed above) through the device. Upon observing this traffic, the device fails to properly inspect the packet and reloads. Some of the vulnerable inspection engines could be enabled by default. This vulnerability affects software releases 7.0, 7.1, 7.2, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6. (CVE-2012-0353)

Cisco ASA Syslog Message Denial-of-Service Vulnerability

Cisco ASA 5500 series products and Catalyst 6500 ASA Service Modules are prone to a remote denial-of-service vulnerability. This vulnerability exists due to the implementation of a specific Syslog message (message ID 305006). An attacker can exploit this vulnerability by sending a sequence of packets through the device that will trigger the Syslog message to be generated. The generation of the message could trigger the device to reload resulting in denial-of-service conditions. This vulnerability affects software releases 7.0, 7.1, 7.2, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6. (CVE-2012-0355)

Cisco Multiple Products PIM Denial-of-Service Vulnerability

Cisco ASA 5500 series products and Catalyst 6500 ASA Service Modules are prone to a remote denial-of-service vulnerability. This vulnerability exists in the way Protocol Independent Multicast (PIM) is implemented. To exploit this vulnerability, an attacker sends a specially crafted PIM packet to the vulnerable device. When the packet is processed, the exploit is triggered. Please note this vulnerability affects Cisco ASA 5500 Series Products and Catalyst 6500 ASA Service Modules configured only in routed firewall mode and only in single context mode where PIM is enabled. This vulnerability can be triggered only by IPv4 PIM. This vulnerability affects software releases 7.0, 7.1, 7.2, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6. (CVE-2012-0356)

Cisco ASA Threat Detection Denial-of-Service Vulnerability

Cisco ASA 5500 series products and Catalyst 6500 ASA Service Modules are prone to a remote denial-of-service vulnerability when configured with the "Scanning Threat Mode feature" and with "shun" action enabled. These options are not enabled by default. An attacker may exploit this vulnerability by sending specially crafted packets through the affected system in a way that triggers the shun action. Successful exploitation will cause a reload on the affected device. This vulnerability affects software releases 7.0, 7.1, 7.2, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6. (CVE-2012-0354)

Successful exploitation of any of these vulnerabilities could cause the device to reload creating denial-of-service conditions. Cisco has released fixes that mitigate the issue.

Cisco acknowledges that the Cisco PIX Security Appliance may be affected by some of the vulnerabilities stated above. Cisco states that as the PIX has reached end of life and customers are encouraged to upgrade to ASA devices.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Cisco after appropriate testing. To view a complete list of what software fixes to apply, please see [hxxp://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120314-asa](http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120314-asa)
- Consider implementing the workaround provided by Cisco. To view the instructions for this workaround please see [hxxp://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120314-asaclient](http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120314-asaclient)
- Consider temporarily adjusting ASA device configuration until appropriate patches can be applied.

REFERENCES:

Cisco:

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120314-asa>

<http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120314-asaclient>

Security Focus:

<http://www.securityfocus.com/bid/52489>

<http://www.securityfocus.com/bid/52484>

<http://www.securityfocus.com/bid/52488>

<http://www.securityfocus.com/bid/52481>

<http://www.securityfocus.com/bid/52482>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0353>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0354>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0356>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0357>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0358>