



State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

April 9, 2009

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:

SA2009-022

DATE(S) ISSUED:

4/9/2009

SUBJECT:

Multiple Vulnerabilities in Cisco PIX Firewalls and ASA Security Devices

OVERVIEW:

Multiple vulnerabilities have been discovered in Cisco PIX firewalls and ASA devices which are network security solutions that can be implemented to block malicious traffic. These vulnerabilities could allow attackers to gain unauthorized access to vulnerable systems, cause these devices to reload, or submit network traffic which bypasses restrictions that allow or deny access to network resources.

SYSTEMS AFFECTED:

- Cisco PIX/ASA 7.0
- Cisco PIX/ASA 7.1
- Cisco PIX/ASA 7.2
- Cisco PIX/ASA 8.0
- Cisco PIX/ASA 8.1

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:

Six vulnerabilities have been discovered in Cisco PIX firewalls and ASA devices that could allow attackers to take complete control of a vulnerable system.

The first vulnerability may allow an attacker to gain unauthorized access to a vulnerable system by bypassing user authentication. The second vulnerability could result in the bypassing of access control lists. Four more vulnerabilities exist that may cause affected devices to reload, thus producing a denial of service condition. Details of these vulnerabilities are as follows:

Authentication Bypass

- An authentication-bypass vulnerability that affects the VPN override account feature would allow an attacker to bypass the configuration options from an AAA server for a WebVPN tunnel.

ACL Bypass

- An access control list vulnerability may be exploited remotely, without authentication, and may allow traffic to bypass firewall devices that use the *implicit deny* access rule at the end of the access control list (ACL). It should be noted that access control lists with *explicit deny* statements are not affected by this vulnerability. You are only affected if you rely on the *implicit deny* at the end of an ACL applied to a device should you not have an *explicit deny* in place.

Denial of Service

- A security vulnerability in ASA devices may be exploited by sending a specially crafted SSL or HTTP packet to an affected device. This vulnerability exists only when devices are configured to terminate SSL VPN connections or have an interface with ASDM access enabled. This could allow a remote attacker to cause a denial of service condition by forcing the affected devices to reload.
- A security vulnerability in PIX and ASA devices may be exploited by specially crafted TCP packets. Cisco ASA devices configured for any of the following services are affected:
 - SSL VPNs
 - ASDM Administrative Access
 - Telnet & SSH Access
 - cTCP for Remote Access VPNs
 - Virtual Telnet & HTTP
 - TLS Proxy for Encrypted Voice Inspection
 - Cut-Through Proxy for Network Access
 - TCP Intercept

This vulnerability could allow a remote attacker to cause a denial of service condition and reload the affected devices.

- A security vulnerability in PIX and ASA devices, configured with SQL *Net Inspection, may be exploited by specially crafted SQL *Net packets being sent over port 1521/TCP. This vulnerability could allow a remote attacker to reload the affected device, resulting in a denial of service condition.
- A security vulnerability in PIX devices may be exploited by sending specially crafted H.323 packets to an affected firewall. This vulnerability could allow a remote attacker to cause a denial of service condition and cause the affected devices to reload.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Cisco to vulnerable systems immediately after appropriate testing.
- Implement strong Access Control Lists which utilize *explicit deny* statements at the end of the ACL.

REFERENCES:

Security Focus:

<http://www.securityfocus.com/bid/34429>

Cisco:

http://www.cisco.com/en/US/products/products_security_advisory09186a0080a994f6.shtml#@ID

http://www.cisco.com/en/US/products/products_applied_mitigation_bulletin09186a0080a99518.html

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1155>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1156>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1157>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1158>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1159>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1160>

US-CERT:

http://www.us-cert.gov/current/index.html#cisco_releases_security_advisory_for9