

[Full-disclosure] Cisco Security Advisory: Multiple Vulnerabilities in Cisco PIX and ASA Appliances

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-10/msg00512.html>

- *From:* Cisco Systems Product Security Incident Response Team <psirt@xxxxxxxx>
 - *Date:* Wed, 17 Oct 2007 13:15:25 -0400
-

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Cisco Security Advisory: Multiple Vulnerabilities in Cisco PIX and ASA Appliances

Advisory ID: cisco-sa-20071017-asa

<http://www.cisco.com/warp/public/707/cisco-sa-20071017-asa.shtml>

Revision 1.0

For Public Release 2007 October 17 1600 UTC (GMT)

+-----

Summary

=====

Two crafted packet vulnerabilities exist in the Cisco PIX 500 Series Security Appliance (PIX) and the Cisco 5500 Series Adaptive Security Appliance (ASA) that may result in a reload of the device. These vulnerabilities are triggered during processing of Media Gateway Control Protocol (MGCP) packets, or during processing of Transport Layer Security (TLS) traffic that terminates on the PIX or ASA security appliance.

Note: These vulnerabilities are independent of each other; a device may be affected by one and not by the other.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20071017-asa.shtml>.

Affected Products

=====

Vulnerable Products

+-----

The Cisco PIX and ASA security appliances are affected by a crafted MGCP packet vulnerability if MGCP application layer protocol inspection is enabled and the device is running certain 7.x software versions. Version 6.3.x is not affected. MGCP inspection is not enabled by default. For specific affected versions, refer to the "Software Versions and Fixes" section.

The PIX and ASA security appliances are also affected by a crafted TLS packet vulnerability that affects devices running certain 7.x software versions if the software has one or more features configured that cause TLS sessions to terminate on the PIX or ASA security appliance. These functions include, but are not limited to, clientless WebVPN, HTTPS management, cut-through proxy for network access, and TLS proxy for encrypted voice inspection. Version 6.3.x is not affected. Features that cause TLS sessions to terminate on the PIX and ASA security appliances are not enabled by default. For specific affected versions, please refer to the "Software Versions and Fixes" section.

In addition to the PIX and ASA security appliances, the crafted MGCP packet vulnerability also affects the Cisco Firewall Services Module (FWSM). More information regarding the FWSM can be found in the companion advisory <http://www.cisco.com/warp/public/707/cisco-sa-20071017-fwsm.shtml>.

To determine whether you are running a vulnerable version of Cisco PIX or ASA software, issue the "show version" command-line interface (CLI) command.

The following example shows a Cisco ASA Security Appliance that runs software release 7.2(3):

```
ASA# show version
```

```
Cisco Adaptive Security Appliance Software Version 7.2(3)
```

```
[...]
```

Customers who use the Cisco Adaptive Security Device Manager (ASDM) to manage their devices can find the version of the software displayed in the table in the login window or in the upper left corner of the ASDM window. The version notation is similar to this:

```
PIX Version 7.2(3)
```

```
Products Confirmed Not Vulnerable
```

```
+-----
```

With the exception of the FWSM, no other Cisco products are known to be vulnerable to the issues described in this advisory.

Details

=====

This Security Advisory describes two distinct vulnerabilities that are independent of each other.

1. Crafted MGCP Packet

A PIX or ASA security appliance with the Media Gateway Control Protocol (MGCP) application layer protocol inspection feature enabled may reload when the device processes a crafted MGCP packet. MGCP application layer protocol inspection is not enabled by default.

MGCP messages are transmitted over the User Datagram Protocol (UDP), which does allow the crafted MGCP messages to be sourced from a spoofed address. Only the MGCP for gateway application (MGCP traffic on UDP port 2427) is affected.

To determine whether MGCP inspection is configured on the PIX or ASA, log in to the device and issue the CLI command "show service-policy | include mgcp". If the output contains the text "Inspect: mgcp" and some statistics, then the device has a vulnerable configuration. The following example shows a vulnerable Cisco ASA Security Appliance:

```
ASA# show service-policy | include mgcp
Inspect: mgcp, packet 15, drop 0, reset-drop 0
ASA#
```

This vulnerability is documented in Cisco Bug ID CSCsi90468. The corresponding Cisco Bug ID for the FWSM, included in the companion FWSM Security Advisory, is CSCsi00694.

2. Crafted TLS Packet

Transport Layer Security (TLS) is the replacement for the Secure Socket Layer (SSL) protocol. It is a protocol that provides, via cryptography, secure communications between two end-points.

The PIX and ASA security appliances rely on TLS to protect the confidentiality of communications in a variety of scenarios. In all these scenarios, the PIX and ASA may be affected by a vulnerability in the handling of the TLS protocol that may lead to a reload of the device when it processes specially crafted TLS packets.

The scenarios affected by this vulnerability are clientless WebVPN connections, HTTPS management sessions, cut-through proxy for network access, and TLS proxy for encrypted voice inspection.

Clientless WebVPN Connections

~~~~~

Clientless WebVPN connections are enabled via the "webvpn" command. For

example, the following configuration shows an ASA running 8.0 software with clientless WebVPN configured and enabled. In this case the ASA will listen for WebVPN connections on the default port, TCP port 443:

```
http server enable
!
webvpn
enable outside
```

Note that with this particular configuration, the device is vulnerable to attacks coming from the outside interface.

#### HTTPS Management Sessions

~~~~~

HTTPS management sessions are enabled via the "http server enable" and "http" commands. For example, the following configuration shows an ASA configured for remote HTTPS management:

```
http server enable
http 192.168.0.0 255.255.255.0 inside
```

Note that with this particular configuration the device is vulnerable to attacks coming from the *inside* interface and from the 192.168.0.0/ 24 IP sub-network.

Cut-Through Proxy for Network Access

~~~~~

The cut-through proxy feature is used to authenticate users before they can access the network. A configuration that requires users to authenticate before they can be granted network access looks like the following example:

```
access-list auth-proxy extended permit tcp any any eq www
access-list auth-proxy extended permit tcp any any eq telnet
access-list auth-proxy extended permit tcp any any eq https
!
aaa authentication match auth-proxy inside LOCAL
aaa authentication secure-http-client
aaa authentication listener https inside port https
```

A configuration affected by this vulnerability will contain the command "aaa authentication secure-http-client" or "aaa authentication listener https inside port <port number>".

Note that with the particular configuration in the preceding example, the device is vulnerable to attacks coming from the \*inside\* interface.

#### TLS Proxy for Encrypted Voice Inspection

~~~~~

This feature allows the security appliance to decrypt, inspect and modify (as needed, for example, performing NAT fixup), and re-encrypt

voice signaling traffic while all of the existing VoIP inspection functions for Skinny and Session Initiation Protocol (SIP) protocols are preserved. Once voice signaling is decrypted, the plain-text signaling message is passed to the existing inspection engines. The security appliance accomplishes this by acting as a TLS proxy between the IP phone and Cisco Unified CallManager, which implies that TLS sessions are terminating on the security appliance.

To determine whether the Cisco PIX or ASA security appliance is configured to support inspection of encrypted voice, log in to the device and issue the CLI command "show service-policy | include tls". If the output contains the text "tls-proxy: active" and some statistics, then the device has a vulnerable configuration. The following example shows a vulnerable Cisco ASA Security Appliance:

```
ASA# show service-policy | include tls
Inspect: sip tls-proxy myproxy, packet 0, drop 0, reset-drop 0
tls-proxy: active sess 0, most sess 0, byte 0
Inspect: skinny tls-proxy myproxy, packet 0, drop 0, reset-drop 0
tls-proxy: active sess 0, most sess 0, byte 0
ASA#
```

This vulnerability is documented in Cisco Bug IDs CSCsg43276 and CSCsh97120. This vulnerability does not affect the FWSM.

Vulnerability Scoring Details

+-----

Cisco is providing scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

Cisco will provide a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

CVSS is a standards-based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided an FAQ to answer additional questions regarding CVSS at:

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at

<http://intellishield.cisco.com/security/alertmanager/cvss>.

Crafted MGCP packet causes PIX/ASA to reload (CSCsi90468)

[Full-disclosure] Cisco Security Advisory: Multiple Vulnerabilities in Cisco PIX and ASA Appliances

CVSS Base Score – 7.1
Access Vector – Network
Access Complexity – Medium
Authentication – None
Confidentiality Impact – None
Integrity Impact – None
Availability Impact – Complete

CVSS Temporal Score – 5.9
Exploitability – Functional
Remediation Level – Official-Fix
Report Confidence – Confirmed

Crafted TLS packet causes PIX/ASA to reload (CSCsg43276 and CSCsh97120)

CVSS Base Score – 7.8
Access Vector – Network
Access Complexity – Low
Authentication – None
Confidentiality Impact – None
Integrity Impact – None
Availability Impact – Complete

CVSS Temporal Score – 6.4
Exploitability – Functional
Remediation Level – Official-Fix
Report Confidence – Confirmed

Impact
=====

Successful exploitation of the vulnerabilities described in this advisory will result in a reload of the affected device. Repeated exploitation can result in a sustained denial of service (DoS) condition.

Software Versions and Fixes
=====

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

[Full-disclosure] Cisco Security Advisory: Multiple Vulnerabilities in Cisco PIX and ASA Appliances

The following list contains the first fixed software release of each vulnerability:

| Affected | First | Vulnerability | Major | Fixed | Release | Release |
|----------|--------------|---------------|--------|-------|---------|----------------------|
| 7.0 | 7.0 | (6.33) | | | | or later |
| 7.1 | Crafted MGCP | 7.1 | (2.54) | | | packet. or later |
| 7.2 | 7.2 | (2.23) | | | | or later |
| 8.0 | 8.0 | (2) | | | | |
| 7.0 | Not | | | | | Affected |
| 7.1 | 7.1 | (2.55) | | | | Crafted TLS or later |
| 7.2 | 7.2 | (2.24) | | | | or later |
| 8.0 | Not | | | | | Affected |

The following maintenance software releases are the first software releases that contain the fixes for the two vulnerabilities mentioned in this Security Advisory: 7.0(7), 7.1(3), 7.2(3), and 8.0(2).

Fixed PIX software can be downloaded from
<http://www.cisco.com/cgi-bin/tablebuild.pl/pix?psrtdcat20e2>.

Fix ASA software can be downloaded from
<http://www.cisco.com/cgi-bin/tablebuild.pl/asa?psrtdcat20e2>.

Workarounds
=====

General Considerations

Filters that deny TLS packets using TCP port 443 and MGCP packets on UDP port 2427 should be deployed throughout the network as part of a transit ACL (tACL) policy for protection of traffic which enters the network at ingress access points. This policy should be configured to protect the network device where the filter is applied and other devices behind it. Filters for TLS packets using TCP port 443 and MGCP packets on UDP port 2427 should also be deployed in front of vulnerable network devices so that traffic is only allowed from trusted clients.

Additional information about tACLs is available in "Transit Access Control Lists : Filtering at Your Edge":

http://www.cisco.com/en/US/tech/tk648/tk361/technologies_white_paper09186a00801afc76.shtml.

Additional mitigations techniques that can be deployed on Cisco devices within the network are available in the Cisco Applied Intelligence companion document for this advisory:

<http://www.cisco.com/warp/public/707/cisco-air-20071017-asafwsm.shtml>.

1. Crafted MGCP Packet

There is no workaround for this vulnerability other than disabling MGCP application layer protocol inspection on the device.

Leveraging anti-spoofing techniques will help mitigate spoofed packets from triggering this vulnerability.

Limiting MGCP application layer inspection to traffic between MGCP gateways may help to mitigate this vulnerability since it would require an attacker to have additional information (the addresses of the MGCP gateways) to launch a successful attack. To limit MGCP application layer inspection to traffic between certain devices, a class map that matches only traffic between the gateways must be created. Then, MGCP inspection must be performed on traffic in that class. The following example shows how to accomplish this:

```
ASA(config)# access-list mgcp_traffic permit udp host 192.168.0.1
host 172.16.0.1 eq 2427
ASA(config)# access-list mgcp_traffic permit udp host 172.16.0.1
host 192.168.0.1 eq 2427
ASA(config)# class-map MGCP
ASA(config-cmap)# match access-list mgcp_traffic
ASA(config-cmap)# exit
ASA(config)# policy-map global_policy
ASA(config-pmap)# class inspection_default
ASA(config-pmap-c)# no inspect mgcp
ASA(config-pmap-c)# exit
ASA(config-pmap)# class MGCP
```

```
ASA(config-pmap-c)# inspect mgcp
ASA(config-pmap-c)# exit
ASA(config-pmap)# exit
ASA(config)#
```

Note that MGCP inspection is applied only to UDP traffic between hosts 192.168.0.1 and 172.16.0.1

See the Cisco Applied Intelligence companion document for additional mitigation possibilities.

2. Crafted TLS Packet

ASDM is used to manage the Cisco PIX or ASA security appliance. Access to ASDM should be allowed only on trusted interfaces and only from authorized hosts. Restricting ASDM access to trusted hosts limits the ability of an attacker to conduct these attacks.

For example, to limit ASDM access to a single host on the inside interface with an address of 192.168.1.2, enter the following command:

```
hostname(config)# http 192.168.1.2 255.255.255.255 inside
```

Additional information is available at:

Cisco Security Appliance Command Line Configuration Guide, Version 7.2
(<http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/mgaccess.html#wp1047288>)

There are no workarounds if the clientless WebVPN, cut-through proxy for network access, and TLS proxy for encrypted voice inspection features are in use.

Obtaining Fixed Software

=====

Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@xxxxxxxx" or "security-alert@xxxxxxxx" for software upgrades.

Customers with Service Contracts

+-----

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

Customers using Third Party Support Organizations

+-----

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

Customers without Service Contracts

+-----

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- * +1 800 553 2447 (toll free from within North America)
- * +1 408 526 7209 (toll call from anywhere in the world)
- * e-mail: tac@xxxxxxxxx

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

Exploitation and Public Announcements

=====

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerabilities described in this advisory.

These vulnerabilities were discovered by Cisco internal testing and customer service requests.

Status of this Notice: FINAL

=====

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

Distribution

=====

This advisory is posted on Cisco's worldwide website at:

<http://www.cisco.com/warp/public/707/cisco-sa-20071017-asa.shtml>

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- * cust-security-announce@xxxxxxxxx
- * first-teams@xxxxxxxxx
- * bugtraq@xxxxxxxxxxxxxxxxxxxxx
- * vulnwatch@xxxxxxxxxxxxxxxxx
- * cisco@xxxxxxxxxxxxxxxxxxxxx
- * cisco-nsp@xxxxxxxxxxxxxxxxxxxxx
- * full-disclosure@xxxxxxxxxxxxxxxxxxxxx
- * comp.dcom.sys.cisco@xxxxxxxxxxxxxxxxxxxxx

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

Revision History

=====

| Revision | Initial |
|----------|-------------------------------------|
| 1.0 | 2007-October-17 public release. |

Cisco Security Procedures

=====
Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

+-----
All contents are Copyright 2006-2007 Cisco Systems, Inc. All rights reserved.
+-----

Updated: Oct 17, 2007 Document ID: 98711
+-----

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.6 (GNU/Linux)

iD8DBQFHFjlY8NUAbBmDaxQRAmb8AJ4n4iDQ/u51DbLAIAX9mr9WCVSdACdGwa3
D59zNDwKMJeaqwWbPsVv5E4=
=Tt21

-----END PGP SIGNATURE-----

Full-Disclosure - We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia - <http://secunia.com/>