

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

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-10/msg00266.html>

---

- *From:* Cisco Systems Product Security Incident Response Team <[psirt@xxxxxxxx](mailto: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

+-----

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

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.