

[NEWS] Multiple Vulnerabilities in Cisco PIX and ASA Appliances

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00063.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 20 Feb 2007 14:08:13 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Multiple Vulnerabilities in Cisco PIX and ASA Appliances

SUMMARY

Multiple vulnerabilities are found in Cisco PIX 500 Series Security Appliances and the Cisco ASA 5500 Series Adaptive Security Appliances. They affect the following:

- * Enhanced inspection of Malformed Hypertext Transfer Protocol (HTTP) traffic
- * Inspection of malformed Session Initiation Protocol (SIP) packets
- * Inspection of a stream of malformed Transmission Control Protocol (TCP) packets
- * Privilege escalation

These vulnerabilities are independent of each other. If a vulnerability affects a device, it does not necessarily mean that the device is affected by all of them.

DETAILS

Affected Products:

In addition to the Cisco PIX 500 Series Security Appliances and the Cisco

[NEWS] Multiple Vulnerabilities in Cisco PIX and ASA Appliances

ASA 5500 Series Adaptive Security Appliances, some vulnerabilities also affect Cisco Firewall Services Module (FWSM). More information regarding FWSM can be found in the companion advisory

<<http://www.cisco.com/warp/public/707/cisco-sa-20070214-fwsm.shtml>>
<http://www.cisco.com/warp/public/707/cisco-sa-20070214-fwsm.shtml>.

Products Confirmed Not Vulnerable:

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

Details:

This Security Advisory describes multiple distinct vulnerabilities. They are independent of each other.

1. Enhanced inspection of Malformed HTTP traffic

Cisco PIX and ASA Security Appliances may crash when inspecting a malformed HTTP request when enhanced HTTP inspection is enabled. If enhanced HTTP application inspection is enabled your configuration will contain a line like "inspect http <appfw>" where <appfw> is the name of a specific HTTP map. Please note that regular HTTP inspection (configured via the command "inspect http" without an HTTP map) is not affected by this vulnerability. This vulnerability affects only 7.x software releases.

For information on what enhanced inspection of HTTP traffic does, and how to configure it, refer to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_7_2/conf_gd/firewall/inspect.htm#wp1431359>
http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_7_2/conf_gd/firewall/inspect.htm#wp1431359

This vulnerability is documented in Cisco Bug ID

<<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd75794>>
CSCsd75794 (registered customers only).

2. Inspection of malformed SIP packets

The inspection of a malformed SIP packet may crash Cisco PIX and ASA appliances. In order to trigger this vulnerability, SIP fixup (for 6.x software) or inspect (for 7.x software) feature must be enabled. SIP fixup is enabled by default in the 6.x software releases, and SIP inspection is disabled by default in the 7.x and later software releases.

This vulnerability is documented in Cisco Bug IDs

<<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsd97077>>
CSCsd97077 (registered customers only) and
<<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCse27708>>
CSCse27708 (registered customers only).

3. Inspection of a stream of malformed TCP packets

By processing a stream of malformed packet in a TCP-based protocol Cisco PIX and ASA Appliances may crash. Processing of the protocol must be done by inspect feature. The packets can be addressed to the device itself or just transiting it. Cisco PIX and ASA Appliance can inspect the following TCP-based protocols:

[NEWS] Multiple Vulnerabilities in Cisco PIX and ASA Appliances

- * Computer Telephony Interface Quick Buffer Encoding (CITQBE)
- * Distributed Computing Environment/Remote Procedure Call (DCE/RPC)
- * Domain Name Service (DNS)
- * Extended Simple Mail Transfer Protocol (ESMTP)
- * File Transfer Protocol (FTP)
- * H.323 protocol
- * Hyper Text Transfer Protocol (HTTP)
- * Internet Locator Server (ILS)
- * Instant Messaging (IM)
- * Point-to-Point Tunneling Protocol (PPTP)
- * Remote Shell (RSH)
- * Real Time Streaming Protocol (RTSP)
- * Session Initiation Protocol (SIP)
- * Skinny (or Simple) Client Control Protocol (SCCP)
- * Simple Mail Transfer Protocol (SMTP)
- * Oracle SQL*Net
- * Sun RPC

This vulnerability is documented in Cisco Bug ID

<<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh12711>>
CSCsh12711 (registered customers only).

4. Privilege escalation

Using the LOCAL method for user authentication may result in privilege escalation. In order to exploit this vulnerability, a user must be defined in the local database with a privilege of zero and be able to successfully authenticate to the affected device. Only if these conditions are met can the user escalate assigned privileges to level 15 and become an administrator. After that, the user can change every aspect of the configuration and operation of the device.

A device is vulnerable to this issue if these lines are present in the device's configuration:

```
pixfirewall(config)# aaa authentication enable console LOCAL
pixfirewall(config)# username <user_name> password <secret_pwd>
privilege 0
```

This vulnerability is documented in Cisco Bug ID

<<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsh33287>>
CSCsh33287 (registered customers only).

Impact:

Successful exploitation of the first three vulnerabilities listed in this Advisory may crash the affected device. Repeated exploitation can result in a sustained DoS attack.

Successful exploitation of CSCsh33287 can result in the escalation of user privileges and complete compromise of the affected Cisco PIX and ASA Appliances.

[NEWS] Multiple Vulnerabilities in Cisco PIX and ASA Appliances

Workarounds:

For vulnerabilities that involve HTTP and SIP protocols, it is possible to apply mitigation techniques. Workarounds are available for the other two vulnerabilities.

Additional mitigations 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-20070214-firewall.shtml>
<http://www.cisco.com/warp/public/707/cisco-air-20070214-firewall.shtml>

Enhanced inspection of Malformed HTTP traffic

Disabling HTTP application inspection (appfw) will prevent Cisco PIX and ASA Appliances from being vulnerable to the issue listed in this Advisory. By leaving inspect http statement configured, some level of protection for the end devices (for example, computers protected by Cisco PIX and ASA Appliance) will remain. However, since this level of inspection is less granular, it may have negative impact on devices terminating HTTP sessions. Devices which terminate HTTP sessions may be exposed to packets that may cause these devices to crash or become compromised.

Inspection of malformed SIP packets

Disabling SIP inspection will prevent Cisco PIX and ASA Appliances from being vulnerable to the issue listed in this Advisory. However, this may have a negative impact on end devices terminating SIP sessions. Devices which terminate SIP sessions could be exposed to packets that may cause these devices to crash or become compromised.

If you run a 7.x software release, the alternative is to only allow traffic from trusted hosts. The configuration needed to accomplish this is as follows.

```
access-list sip-acl extended permit udp 10.1.1.0 255.255.255.0 host
192.168.5.4 eq sip
access-list sip-acl extended permit udp host 192.168.5.4 10.1.1.0
255.255.255.0 eq sip
```

```
class-map sip-traffic
match access-list sip-acl
!
!
policy-map global_policy
class inspection_default
inspect dns maximum-length 512
inspect ftp
inspect h323 h225
inspect h323 ras
inspect rsh
inspect rtsp
```

[NEWS] Multiple Vulnerabilities in Cisco PIX and ASA Appliances

```
inspect esmtp
inspect sqlnet
inspect skinny
inspect sunrpc
inspect xdmcp
inspect netbios
inspect tftp
class sip-traffic
inspect sip
!
service-policy global_policy global
```

In this example, the SIP endpoints are any host within the 10.1.1.0 network (inside the trusted network) and a host with the IP address of 192.168.5.4 (outside of the trusted network). You have to substitute these IP addresses with the ones that are used in your network.

Note that SIP is an UDP-based protocol, so spoofing SIP messages is possible.

Inspection of a stream of malformed TCP packets

The workaround is to increase the minimum TCP segment size (MSS) to 64. This is accomplished with a global `sysopt` command:

```
sysopt connection tcpmss minimum 64
```

Privilege escalation

There are two workarounds for this vulnerability. One consists of the use of TACACS+ or Radius for authentication, and another is to change the minimum privilege of the user from zero to one.

Use TACACS+ or Radius for authentication

Do not use the LOCAL method for user authentication, but use TACACS+ or Radius instead. This example shows how to configure the Cisco PIX appliance to use TACACS+ or Radius to authenticate Secure Shell (SSH) access to the device.

```
pixfirewall(config)#aaa-server AuthOutbound protocol radius (or
tacacs+)
pixfirewall(config)#aaa authentication ssh console AuthOutbound
pixfirewall(config)#aaa-server AuthOutbound host 10.0.0.1 <radius_key>
```

In this example, 10.0.0.1 is the IP address of the Radius server and `radius_key` is the shared key between the Radius server and the appliance.

More information on how to configure TACACS+ or Radius on Cisco PIX and ASA appliances can be found at

http://cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a00807349e7.shtml>
http://cisco.com/en/US/products/hw/vpndevc/ps2030/products_configuration_example09186a00807349e7.shtml.

[NEWS] Multiple Vulnerabilities in Cisco PIX and ASA Appliances

Changing user's minimum privilege level

The second workaround consists of the change of the user minimum privilege level from zero to one. In that case, your configuration may look like this:

```
pixfirewall(config)# aaa authentication enable console LOCAL
pixfirewall(config)# username <user_name> password <secret_pwd>
privilege 1
```

It is possible to use any other level as long as it is not zero or 15. If it is 15, the user has all privileges, and that is what we want to avoid in the first place.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:psirt@xxxxxxxx>> Cisco Systems Product Security Incident Response Team.

The original article can be found at:

<<http://www.cisco.com/warp/public/707/cisco-sa-20070214-pix.shtml>>
<http://www.cisco.com/warp/public/707/cisco-sa-20070214-pix.shtml>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.