

Cisco Security Advisory: LDAP and VPN Vulnerabilities in PIX and ASA Appliances

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2007-05/msg00021.html>

- *From:* Cisco Systems Product Security Incident Response Team <psirt@xxxxxxxx>
 - *Date:* Wed, 02 May 2007 17:30:00 -0000
-

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

Hash: SHA1

Cisco Security Advisory: LDAP and VPN Vulnerabilities in PIX and ASA Appliances

Advisory ID: cisco-sa-20070502-asa

<http://www.cisco.com/warp/public/707/cisco-sa-20070502-asa.shtml>

Revision 1.0

Last Updated 2007 May 02 1600 UTC (GMT)

For Public Release 2007 May 02 1600 UTC (GMT)

Contents

=====

Summary
Affected Products
Details
Vulnerability Scoring Details
Impact
Software Version Fixes
Workarounds
Obtaining Fixed Software
Exploitation and Public Announcements
Status of this Notice: FINAL
Distribution
Revision History
Cisco Security Procedures

Cisco Security Advisory: LDAP and VPN Vulnerabilities in PIX and ASA Appliances

Summary

=====

Multiple vulnerabilities exist in the Cisco Adaptive Security Appliance (ASA) and PIX security appliances. These vulnerabilities include two Lightweight Directory Access Protocol (LDAP) authentication bypass vulnerabilities and two denial of service (DoS) vulnerabilities.

The Lightweight Directory Access Protocol (LDAP) authentication bypass vulnerabilities are caused by a specific processing path followed when the device is setup to use a Lightweight Directory Access Protocol (LDAP) authentication server. These vulnerabilities may allow unauthenticated users to access either the internal network or the device itself.

The two DoS vulnerabilities may be triggered when devices are terminating Virtual Private Networks (VPN). These denial of service vulnerabilities may allow an attacker to disconnect VPN users, prevent new connections, or prevent the device from transmitting traffic.

These vulnerabilities are distributed in the authentication, IPsec VPN, and SSL VPN code. They are categorized in this advisory by their Cisco bug descriptions:

- * LDAP Authentication Bypass
- * Denial of Service in VPNs with Password Expiry
- * Denial of Service in SSL VPNs

Cisco has made free software available to address these vulnerabilities for affected customers.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070502-asa.shtml>

Affected Products

=====

Vulnerable Products

+-----+

Cisco ASA and PIX security appliances that are running software versions 7.1 and 7.2 may be vulnerable. To identify the vulnerable versions for a specific issue, please consult the table below.

+-----+

| | Affected |
| Vulnerability | Software |

Cisco Security Advisory: LDAP and VPN Vulnerabilities in PIX and ASA Appliances

Version
LDAP Authentication 7.2 versions bypass prior to 7.2(2)8
7.1 versions Denial of Service in prior to VPNs with password 7.1(2)49 expiry 7.2 versions prior to 7.2(2)17
7.1 versions prior to Denial of Service in 7.1(2)49 SSL VPNs 7.2 versions prior to 7.2(2)19

To determine the version of Cisco ASA or PIX system software your device is running, log into command line interface (CLI) of the device and issue the show version command.

This example shows an ASA that runs software release 7.2(2)10:

```
ciscoasa# show version
```

```
Cisco Adaptive Security Appliance Software Version 7.2(2)10
```

For customers that manage their devices through the Cisco Adaptive Security Device Manager (ASDM), log into the application, and the version can be found either in the table in the login window or in the upper left hand corner of the ASDM window indicated by a label similar to:

```
PIX Version 7.2(2)10
```

Cisco ASA and PIX security appliances running affected software version are only vulnerable if they are running one of the following configurations:

LDAP Authentication Bypass Vulnerability

Two configuration scenarios exist where Cisco PIX or ASA devices are vulnerable:

* Layer 2 Tunneling Protocol (L2TP)

Cisco Security Advisory: LDAP and VPN Vulnerabilities in PIX and ASA Appliances

Devices configured to use a LDAP authentication server and use an authentication protocol other than PAP may be vulnerable. The LDAP server is specified in the configuration via the `aaa-server ldap server host <ip address>` command line interface (CLI) configuration command. The authentication protocol is specified via the `authentication <protocol>` command within the `tunnel-group <tunnel-group> ppp-attributes` section of the configuration.

Relevant configuration segments of a vulnerable device are shown below. In the following example configuration, the authentication server is specified as LDAP and the authentication protocol is specified as `ms-chap-v2`:

```
aaa-server ldap_server protocol ldap
aaa-server ldap_server host 192.168.1.100
timeout 5
ldap-scope onelevel
```

```
tunnel-group example_12tp_group general-attributes
address-pool inside_addresses
authentication-server-group ldap_server
```

```
tunnel-group example_12tp_group ppp-attributes
authentication ms-chap-v2
```

* Remote Management Access

Devices configured to allow remote management access (telnet, SSH, HTTP) and use LDAP authentication, authorization, accounting (AAA) server for credential validation may be vulnerable.

In the configuration file, the `server_group` is defined as a LDAP server with the command `aaa-server <server_group> protocol ldap`. The LDAP authentication server for remote management access is defined via the command, `aaa authentication {telnet | ssh | http | serial} console server_group`.

Relevant configuration segments of a vulnerable device are shown below. The authentication server is specified as LDAP, and remote management access for SSH is permitted and credentials checked by the defined LDAP AAA server:

```
ssh 192.168.1.2 255.255.255.255 inside
```

```
aaa-server ldap_server protocol ldap
aaa-server ldap_server host 192.168.1.100
timeout 5
ldap-scope onelevel
aaa authentication ssh console ldap_server
```

Denial of Service in VPNs with Password Expiry

A device may be affected by this vulnerability if the password-management command is present in the tunnel-group section, as shown in the following examples:

```
tunnel-group example_group general-attributes
address-pool inside_addresses
default-group-policy example_group
password-management
```

```
tunnel-group example_group general-attributes
address-pool inside_addresses
default-group-policy example_group
password-management password-expire-in-days 30
```

Denial of Service in SSL VPNs

Clientless SSL VPNs must be enabled on an interface in order for the device to be affected by this vulnerability.

Devices with clientless SSL VPNs enabled have a webvpn section in the running configuration. This will be similar to the following entry:

```
webvpn
enable outside
url-list ServerList "WSHAWLAP" cifs://10.2.2.2 1
url-list ServerList "FOCUS_SRV_1" https://10.2.2.3 2
url-list ServerList "FOCUS_SRV_2" http://10.2.2.4 3
```

Products Confirmed Not Vulnerable

The Firewall Services Module (FWSM) is not affected by any of the vulnerabilities disclosed in this advisory.

Cisco ASA and PIX security appliances are not affected by these vulnerabilities under the following conditions:

LDAP Authentication Bypass for L2TP Sessions

ASA and PIX security appliances with the following configurations are not affected by this vulnerability:

Cisco Security Advisory: LDAP and VPN Vulnerabilities in PIX and ASA Appliances

- * Devices configured for L2TP over IPsec and using an authentication server other than LDAP
- * Devices configured for L2TP over IPsec and using a LDAP authentication server with PAP
- * Devices using AAA server other than LDAP or a local database for authentication of remote management sessions

Denial of Service in VPNs with Password Expiry

+-----

Device without remote access tunnel groups configured with password expiry are not susceptible to this vulnerability.

Denial of Service in SSL VPNs

+-----

Devices not configured to support clientless SSL VPN connections are not susceptible to this vulnerability. PIX Security Appliances do not support clientless SSL VPN connections and are not vulnerable.

Details

=====

The PIX is a firewall appliance that delivers user and application policy enforcement, multi-vector attack protection, and secure connectivity services.

The Adaptive Security Appliance (ASA) is a modular platform that provides security and VPN services. The ASA offers firewall, intrusion prevention (IPS), anti-X, and VPN services.

LDAP Authentication Bypass

+-----

Cisco ASA and PIX devices leveraging LDAP AAA servers for authentication of terminating L2TP IPsec tunnels or remote management sessions may be vulnerable to an authentication bypass attack. See the following bullets for more details:

* Layer 2 Tunneling Protocol (L2TP)

Devices terminating L2TP IPsec tunnels must be configured to use LDAP in conjunction with CHAP, MS-CHAPv1, or MS-CHAPv2 authentication protocols to be vulnerable. If LDAP authentication is used in conjunction with PAP, the device is not vulnerable to the LDAP L2TP authentication bypass.

* Remote Management Access

Cisco ASA and PIX devices leveraging LDAP AAA servers for

Cisco Security Advisory: LDAP and VPN Vulnerabilities in PIX and ASA Appliances

authentication of management sessions (telnet, SSH and HTTP) may be vulnerable to an authentication bypass attack. Access for management sessions must be explicitly enabled and is limited to the defined source IP address within the device configuration.

This vulnerability is documented as bug ID CSCsh42793.

Denial of Service in VPNs with Password Expiry

Cisco ASA and PIX devices terminating remote access VPN connections may be vulnerable to a DoS attack if the tunnel group is configured with password expiry. To exploit this vulnerability for IPSec VPN connections, an attacker would need to know the group name and group password. An attacker would not need this information for SSL VPN connections. A successful attack results in a reload of the device.

This vulnerability is documented as software bug CSCsh81111.

Denial of Service in SSL VPNs

Cisco ASAs using clientless SSL VPNs are vulnerable to a denial of service attack via the SSL VPN HTTP server. A successful attack must exploit a race condition in the processing non-standard SSL sessions and results in a reload of the device.

More details are available in bug CSCsi16248.

Vulnerability Scoring Details

Cisco is providing scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS).

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.

Cisco PSIRT will set the bias in all cases to normal. Customers are encouraged to apply the bias parameter when determining the environmental impact of a particular vulnerability.

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 Security Advisory: LDAP and VPN Vulnerabilities in PIX and ASA Appliances

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at <http://intellishield.cisco.com/security/alertmanager/cvss>

Cisco Bug IDs:

CSCsh42793 – LDAP Authentication Bypass for L2TP Sessions

CVSS Base Score: 8.0
Access Vector: Remote
Access Complexity: High
Authentication: Not Required
Confidentiality Impact: Complete
Integrity Impact: Complete
Availability Impact: Complete
Impact Bias: Normal

CVSS Temporal Score: 6.6
Exploitability: Functional
Remediation Level: Official–Fix
Report Confidence: Confirmed

CSCsh42793 – LDAP Authentication Bypass for L2TP Sessions

CVSS Base Score: 3.3
Access Vector: Remote
Access Complexity: Low
Authentication: Not Required
Confidentiality Impact: None
Integrity Impact: None
Availability Impact: Complete
Impact Bias: Normal

CVSS Temporal Score: 2.7
Exploitability: Functional
Remediation Level: Official–Fix
Report Confidence: Confirmed

CSCsi16248 – Denial of Service in SSL VPNs

CVSS Base Score: 3.3
Access Vector: Remote
Access Complexity: Low
Authentication: Not Required
Confidentiality Impact: None
Integrity Impact: None
Availability Impact: Complete
Impact Bias: Normal

Cisco Security Advisory: LDAP and VPN Vulnerabilities in PIX and ASA Appliances

CVSS Temporal Score: 2.7
Exploitability: Functional
Remediation Level: Official-Fix
Report Confidence: Confirmed

Impact

=====

Successful exploitation of the LDAP Authentication bypass vulnerability may allow unauthorized users to access the device or internal resources. The DoS vulnerability in VPN password expiry and the DoS vulnerability in clientless SSL VPNs could be repeatedly exploited to cause an extended DoS condition.

Software Version 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.

First Fixed	Vulnerability	Release
7.1	7.2	
LDAP Authentication Bypass	affected	7.2(2)8
Denial of Service	in	VPNs with Password
		7.1(2)49 7.2(2)17
Denial of Service	in	SSL VPNs
		7.1(2)49 7.2(2)17

More information on how and where to obtain fixed software can be found in the Obtaining Fixed Software section of this advisory.

Workarounds

=====

This section of the advisory describes workarounds that may be useful in some environments. Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Intelligence companion document for this advisory at the following link:

<http://www.cisco.com/warp/public/707/cisco-air-20070502-asa.shtml>

LDAP Authentication bypass

+-----

The following workarounds may be a useful reference for some customers to mitigate the LDAP authentication bypass vulnerabilities.

* L2TP

For Cisco ASA or PIX devices configured to use a LDAP authentication server for L2TP over IPsec connections, configuring the device to use PAP as an authentication protocol may mitigate this vulnerability. It is important to note that PAP transmits passwords in clear-text. PAP authentication is encrypted via IPsec when it is used for the L2TP connection. Communications between the security appliance and the LDAP server are not encrypted by default and can be secured with SSL using the `ldap-over-ssl` command. Configuration of PAP authentication can be done using the following example as a guide or by referring to the security appliance configuration guides listed:

```
ciscoasa# config t
ciscoasa(config)# tunnel-group l2tp_group ppp-attributes
ciscoasa(config-ppp)# authentication pap
ciscoasa(config-ppp)# no authentication ms-chap-v1
ciscoasa(config-ppp)# no authentication ms-chap-v2
ciscoasa(config-ppp)# no authentication chap
```

Information on configuring L2TP over IPSEC using the CLI is available at the following link:

http://www.cisco.com/en/US/partner/products/ps6120/products_configuration_guide_chapter09186a008066ebb6.html

Information on configuring L2TP over IPSEC using the ADSM can be found at:

http://www.cisco.com/en/US/partner/products/ps6121/products_configuration_guide_chapter09186a00806a81bc.html

* Remote Management

Cisco ASA or PIX devices that authenticate remote management sessions with either the local database or an AAA server other than a LDAP

Cisco Security Advisory: LDAP and VPN Vulnerabilities in PIX and ASA Appliances

server are not affected by this vulnerability. More information on changing the AAA server protocol used with remote management sessions is available at the following link:

http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_7_2/conf_gd/sysadmin/mgaccess.htm.

Remote management sessions must be explicitly enabled before the Cisco ASA or PIX will accept sessions. The source IP addresses are defined within the command that enables remote management access. Below are examples of enabling remote management sessions (Note that other commands are required, but these commands control the source IP address of the device that is allowed access to the Cisco ASA or PIX device):

For remote telnet, ssh and http access:

```
ciscoasa# config t
ciscoasa(config)# telnet source_IP_address mask source_interface
ciscoasa(config)# ssh source_IP_address mask source_interface
ciscoasa(config)# http source_IP_address mask source_interface
```

Denial of Service in VPNs with Password Expiry

+-----

Disabling password expiry for remote access users until a device can be updated with non-vulnerable code can prevent the exposure of this vulnerability. This can be accomplished by removing the password management entry in the general attributes of the tunnel group, as shown in the following example:

```
ciscoasa# config t
ciscoasa(config)# tunnel-group remote_access_group general-attributes
ciscoasa(config-tunnel-general)# no password-management
```

Implementing this workaround will disable the password expiry feature, and users will not be forced to change their passwords.

More information on the password-management command is available in the Security Appliance Command reference at the following link:

http://www.cisco.com/en/US/products/ps6120/products_command_reference_chapter09186a008063f0f8.html#wp1725

Denial of Service in SSL VPNs

+-----

If clientless SSL VPNs are used, there is no workaround for the SSL VPN vulnerability. Client-based VPNs are not affected, and may be used as an alternative to the clientless VPN connections.

More information on configuring clientless SSL VPNs on the ASA is available in the configuration example at the following link:

Cisco Security Advisory: LDAP and VPN Vulnerabilities in PIX and ASA Appliances

http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00806ea271.shtml

Obtaining Fixed Software

=====

Cisco will make free software available to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. 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>.

Registered users can download the latest ASA and PIX releases at:
<http://www.cisco.com/cgi-bin/tablebuild.pl/asa-interim>
<http://www.cisco.com/cgi-bin/tablebuild.pl/pix-interim>

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 vulnerability described in this advisory.

These vulnerabilities were reported to Cisco by customers that experienced these issues during normal operation of their equipment.

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

=====

Cisco Security Advisory: LDAP and VPN Vulnerabilities in PIX and ASA Appliances

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

<http://www.cisco.com/warp/public/707/cisco-sa-20070502-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-May-02 | 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>

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

Version: GnuPG v1.4.5 (SunOS)

iD8DBQFGOMmZ8NUAbBmDaxQRAgR0AKCtXa3JeoALzIadeyj6QLqEJD/PmwCcCioq
zyjxRFP1pvkbGTR29LKFzI4=
=358u

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