

Cisco Security Advisory: Unintentional Password Modification in Cisco Firewall Products

Document ID: 70811

Advisory ID: cisco-sa-20060823-firewall

<http://www.cisco.com/warp/public/707/cisco-sa-20060823-firewall.shtml>

Revision 1.0

For Public Release 2006 August 23 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

[Summary](#)

[Affected Products](#)

[Details](#)

[Impact](#)

[Software Version and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of this Notice: FINAL](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

Summary

Certain versions of the software for the Cisco PIX 500 Series Security Appliances, the Cisco ASA 5500 Series Adaptive Security Appliances (ASA), and the Firewall Services Module (FWSM) are affected by a software bug that may cause the EXEC password, passwords of locally defined usernames, and the enable password in the startup configuration to be changed without user intervention.

Unauthorized users can take advantage of this bug to try to gain access to a device that has been reloaded after passwords in its startup configuration have been changed. In addition, authorized users can be locked out and lose the ability to manage the affected device.

Cisco has made free software available to address this issue for affected customers.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20060823-firewall.shtml>.

Affected Products

Cisco PIX 500 Series Security Appliances, the Cisco ASA 5500 Series Adaptive Security Appliances, and the Firewall Services Module (FWSM) for the Cisco Catalyst 6500 Switches and Cisco 7600 Series Routers are impacted if they are running an affected software version.

Vulnerable Products

The PIX 500 Series Security Appliances and the ASA 5500 Series Adaptive Security Appliances are affected when running any of the following software versions:

- Any version (including interim versions) in the 7.0(x) train up to and including 7.0(5)
- Any version (including interim versions) in the 7.1(x) train up to and including 7.1(2.4)

The FWSM for the Cisco Catalyst 6500 Switches and Cisco 7600 Series Routers is affected when running the following software version:

- Any version (including interim versions) in the 3.1(x) train up to and including 3.1(1.6)

Products Confirmed Not Vulnerable

The PIX 500 Series Security Appliances and the ASA 5500 Series Adaptive Security Appliances are *not affected* when running any of the following software versions:

- Any pre-7.x version (PIX only since the ASA does not run pre-7.x code)
- 7.2(1) and later

The FWSM for the Cisco Catalyst 6500 Switches and Cisco 7600 Series Routers is *not affected* when running any of the following software versions:

- Any 1.x and 2.x version
- 3.1(2) and later

No other Cisco products are currently known to be affected by this issue.

Details

The Cisco PIX 500 Series Security Appliances, the Cisco ASA 5500 Series Adaptive Security Appliances, and the Firewall Services Module (FWSM) for the Cisco Catalyst 6500 Switches and Cisco 7600 Series Routers are part of Cisco's security portfolio. All of these products offer firewall services with stateful packet filtering and deep packet inspection. The PIX and ASA devices also offer other services like Virtual Private Networking (VPN), Content Filtering, and Intrusion Prevention.

On these devices, authentication for both EXEC mode and enable mode can be performed based on Authentication, Authorization, and Accounting (AAA) methods (Remote Authentication Dial-In User Service [RADIUS], Terminal Access Controller Access Control System Plus [TACACS+], or LOCAL). If a device does not have any AAA method (i.e., RADIUS, TACACS+, or LOCAL) configured, authentication for EXEC mode is performed using the password configured with the **passwd** command, and authentication for enable mode is performed using the password configured with the **enable password** command.

A software bug exists in certain versions of the software used by these devices that may cause, under some circumstances, the EXEC password, passwords of locally defined users, and the enable password that are stored in the startup configuration to be changed without user intervention. The startup configuration is stored in a non-volatile medium such as flash memory.

The affected passwords are set using the following configuration commands:

- **passwd** – configures the EXEC password. For example:

```
pix(config)# passwd xxxxxxxxx
```

- **username** – configures local users and their associated passwords. For example:

```
pix(config)# username admin password xxxxxxxxx
```

- **enable password** – configures the password used to enter **enable** mode. For example:

```
pix(config)# enable password xxxxxxxxx
```

The software bug is known to be triggered in only two scenarios:

- A software crash, normally caused by a software bug. Please note that not all software crashes may cause the undesired results discussed above.
- Two or more users making concurrent configuration changes on a device, regardless of the method (command–line interface [CLI], Adaptive Security Device Manager [ASDM], Firewall Management Center, etc.) used to access the device.

Please note that the passwords in the startup configuration will be changed when the configuration is saved, to the non–volatile medium where the startup configuration is stored, via the **write memory** or **copy running–config startup–config** commands. During normal operation, if the running configuration is not saved, passwords in the startup configuration will not change.

Once the passwords in the startup configuration are changed, administrators will be locked out after the next device reload if authentication for EXEC and for enable privilege depends on the passwords or local accounts stored in the startup configuration. If a AAA server (RADIUS or TACACS+) is used for authentication, the change of passwords in the startup configuration will only cause the undesired results when the AAA server is unavailable, *regardless* of whether the "LOCAL" authentication method is configured as a fallback, e.g. `aaa authentication enable console RADIUS LOCAL`.

Passwords are changed to a non–random value. This behavior is not due to a hardcoded default password or other explicitly induced set of password values, but rather the result of a coding error related to configuration parsing.

Devices configured in multiple context mode are also affected by this software bug.

This issue is documented in the following Cisco bug IDs:

- [CSCse02703](#) ([registered](#) customers only) for the PIX and ASA devices
- [CSCsd81487](#) ([registered](#) customers only) for the FWSM

Impact

The software issue may cause the EXEC password, password of locally defined users, and the enable password in the startup configuration to change without user's intervention. This will prevent administrators from logging in to the device if authentication is configured to use the passwords stored in the startup configuration.

If a malicious user were able to guess the new password, and the device reloads, either automatically because of a software crash, or manually by the network administrator, unauthorized access to the device may be possible.

Software Version 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.

For version 7.0.x of the PIX/ASA software, the first fixed release is 7.0(5.1). The latest 7.0.x release for the PIX can be downloaded from:

<http://www.cisco.com/cgi-bin/tablebuild.pl/pix?psrtdcat20e2> ([registered](#) customers only)

The latest 7.0.x release for the ASA can be downloaded from:

<http://www.cisco.com/cgi-bin/tablebuild.pl/asa?psrtdcat20e2> ([registered](#) customers only)

For version 7.1.x of the PIX/ASA software, the first fixed release is 7.1(2.5). The latest 7.1.x interim for the PIX can be downloaded from:

<http://www.cisco.com/cgi-bin/tablebuild.pl/pix-interim?psrtdcat20e2> ([registered](#) customers only)

The latest 7.1.x interim for the ASA can be downloaded from:

<http://www.cisco.com/cgi-bin/tablebuild.pl/asa-interim?psrtdcat20e2> ([registered](#) customers only)

The first fixed release of the FWSM is 3.1(2). The latest 3.1 release of the FWSM software can be downloaded from:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cat6000-fwsm?psrtdcat20e2> ([registered](#) customers only)

Note: Interim images are not fully regression tested. Each individual fix has been unit tested, and the image has had a limited amount of automated regression testing to confirm a baseline of functionality. Keep this testing status in mind if you decide to run them in a production environment. We strongly encourage you to upgrade to a fully tested Maintenance or Feature release when it becomes available.

Workarounds

Configuring authentication against an external RADIUS/TACACS+ server, per network security best practices, mitigates this issue. For information on how to configure authentication, please visit the following URLs:

PIX/ASA:

http://www.cisco.com/en/US/products/ps6120/products_configuration_guide_chapter09186a00804512a5.html

FWSM:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_module_configuration_guide_chapter09186a00804512a5.html

If the passwords in the startup configuration have been modified as a result of software crash or concurrent configuration update, the administrators will need to perform a password recovery procedure, unless external AAA authentication is configured.

The password recovery procedure for the PIX and the ASA is documented at the following URL:

http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_password_recovery09186a008009478b.shtml

The password recovery procedure for the FWSM is documented at the following URL:

http://www.cisco.com/en/US/products/hw/switches/ps708/products_module_configuration_guide_chapter09186a008009478b.shtml

In addition, it is possible to limit the exposure of the firewall device by permitting remote connections only from known, trusted IP addresses. This is accomplished via the **ssh**, **telnet**, and **http** commands for Secure Shell (SSH), Telnet, and Secure Hyper-Text Transfer Protocol (HTTPS) access, respectively. For additional information on this, please refer to the "Managing System Access" section of the Cisco Security Appliance CLI Configuration Guide, available at:

http://www.cisco.com/en/US/products/ps6120/products_configuration_guide_chapter09186a0080450d39.html

In the case of the FWSM, please note that remote access to it can also be obtained via the Cisco Catalyst 6500 switch or Cisco 7600 Series router that hosts the FWSM blade. For this reason, the switch or router needs to be configured, using access control lists, to permit remote connections only from known, trusted IP addresses.

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>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" 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@cisco.com

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 issue described in this advisory, although we are aware that some customers have been impacted by this software bug.

This issue was brought to Cisco's attention by Terje Bless from Helse Nord IKT. Cisco would like to thank him for working with us towards coordinated disclosure of this issue.

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-20060823-firewall.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@cisco.com
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net

- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

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 1.0	2006 August 23	Initial 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>.

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Aug 23, 2006

Document ID: 70811
