

# Cisco Security Advisory: SSL/TLS Certificate and SSH Public Key Validation Vulnerability

Document ID: 81583

Advisory ID: cisco-sa-20070118-certs

<http://www.cisco.com/warp/public/707/cisco-sa-20070118-certs.shtml>

## Revision 1.0

For Public Release 2007 January 18 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

The Cisco Security Monitoring, Analysis and Response System (CS-MARS) and the Cisco Adaptive Security Device Manager (ASDM) do not validate the Secure Sockets Layer (SSL)/Transport Layer Security (TLS) certificates or Secure Shell (SSH) public keys presented by devices they are configured to connect to. Malicious users may be able to use this lack of certificate or public key validation to impersonate the devices that these affected products connect to, which could then be used to obtain sensitive information or misreport information.

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

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070118-certs.shtml>.

## Affected Products

The following products are affected by the vulnerability described in this document:

- Cisco Security Monitoring, Analysis and Response System (CS-MARS)

All CS–MARS versions prior to 4.2.3 are affected.

To verify the version of CS–MARS software, log into CS–MARS web interface using a web browser and go to the "Help" tab located on the top–right corner of the browser window. Then click on the "About" link. The CS–MARS version will be displayed in the center of the browser window under "CS–MARS Information".

Alternatively, it is possible to use an SSH connection or a direct serial console connection to verify the version of the CS–MARS software by logging into the system administration command line interface with the **pnadmin** account and executing the **version** command:

```
shell$ ssh pnadmin@10.0.0.1
pnadmin@10.0.0.1's password:
Last login: Mon Jan  8 18:42:45 2007 from 10.0.0.2

    CS MARS - Mitigation and Response System

    ? for list of commands

[pnadmin]$ version
4.2.3 (2403)
```

- Cisco Adaptive Security Device Manager (ASDM)

All ASDM versions prior to 5.2(2.54) are affected when the ASDM Launcher (the stand–alone version of ASDM) is used.

If the ASDM Applet is used, i.e. ASDM is launched via a web browser, then it is the web browser's responsibility to verify the certificates presented by the devices that ASDM connects to. The user can instruct the web browser to save devices' root Certificate Authority certificates so a warning is generated if something changes (this can be used as a workaround – please refer to the Workarounds section for details.)

To verify the version of ASDM software, launch ASDM and look in the "General" tab of the "Device Information" section.

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

## Details

Some Cisco products connect to different devices for configuration or monitoring purposes. The actual connection method used varies depending on the product, but SSL/TLS and SSH are the most prevalent ones due to their use of strong cryptography to ensure the confidentiality and integrity of the communication.

Two examples of these products include the Cisco Security Monitoring, Analysis and Response System (CS–MARS), a security threat mitigation system that talks to devices such as IPS sensors and firewalls, and the Cisco Adaptive Security Device Manager (ASDM), which provides management and monitoring services for the Cisco ASA 5500 Series Adaptive Security Appliances, Cisco PIX 500 Series Security Appliances and the Firewall Services Modules for the Cisco Catalyst 6500 Switches and the Cisco 7600 Series Routers.

When these products connect to their managed devices via SSL/TLS or SSH, they do not validate the SSL/TLS certificates or SSH public keys presented by these managed devices.

Because the certificates and public keys presented by devices are not validated, in the event that a certificate or public key has changed, the affected products will not be able to determine whether the device they are

communicating with is legitimate, or if it is a device impersonating a legitimate one.

The following Cisco Bug IDs are being used to track these vulnerabilities on the affected products:

- CS-MARS – CSCsf95930 ( registered customers only)
- ASDM – CSCsg78595 ( registered customers only)

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

| CSCsf95930 and CSCsg78595  |                   |                |                   |                   |                |                |
|--|-------------------|----------------|-------------------|-------------------|----------------|----------------|
| Calculate the environmental score of CSCsf95930 and CSCsg78595 <a href="#">↗</a> |                   |                |                   |                   |                |                |
| CVSS Base Score – 4.7  |                   |                |                   |                   |                |                |
| Access Vector  | Access            | Authentication | Confidentiality   | Integrity         | Availability   | Impact         |
| Remote   | Complexity<br>Low | Not Required   | Impact<br>Partial | Impact<br>Partial | Impact<br>None | Bias<br>Normal |
| Temporal Score – 3.9   |                   |                |                   |                   |                |                |
| Exploitability   | Remediation Level |                |                   | Report Confidence |                |                |
| Functional   | Official Fix      |                |                   | Confirmed         |                |                |

## Impact

Successful exploitation of this vulnerability may allow an attacker to obtain sensitive information such as login credentials or submit false data to the affected Cisco product by impersonating a managed device, thus impacting the integrity of the affected Cisco product.

## 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.

Cisco Security Advisory: SSL/TLS Certificate and SSH Public Key Validation Vulnerability

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.

This vulnerability is fixed in version 4.2.3 (2403) of the CS-MARS software. CS-MARS software can be downloaded from the following location:

<http://www.cisco.com/cgi-bin/tablebuild.pl/cs-mars?psrtdcat20e2>

This vulnerability is fixed in version 5.2(2.54) of ASDM. ASDM can be downloaded from the following location:

<http://www.cisco.com/cgi-bin/tablebuild.pl/asa-interim?psrtdcat20e2>

**Note:** The ASDM versions for the PIX/ASA and the FWSM are different. A fixed version of the ASDM software for the FWSM is forthcoming. This advisory will be updated when a fixed image for the FWSM version of ASDM is available.

## Workarounds

There are no workarounds for this vulnerability in the case of CS-MARS.

In the particular case of ASDM, using the ASDM Applet, i.e. launching ASDM via a web browser and not via the stand-alone ASDM Launcher, will workaround the vulnerability since the SSL/TLS certificate verification will be performed by the web browser, and in the case that the certificate has changed, the browser will produce a warning. Note that this requires the user to save the root Certificate Authority (CA) certificate as a trusted certificate.

While not a workaround for the affected products, as a security best practice, you should always configure the devices that the affected products connect to so only connections from trusted hosts or networks are accepted. The way to configure this varies depending on the device. Please refer to the documentation of your managed device for details.

## 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](mailto: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 vulnerability described in this advisory.

Cisco would like to thank Jan Bervar from NIL Data Communications for bringing this to our attention.

## 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.

Cisco Security Advisory: SSL/TLS Certificate and SSH Public Key Validation Vulnerability

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-20070118-certs.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](mailto:cust-security-announce@cisco.com)
- [first-teams@first.org](mailto:first-teams@first.org)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [full-disclosure@lists.grok.org.uk](mailto:full-disclosure@lists.grok.org.uk)
- [comp.dcom.sys.cisco@newsgate.cisco.com](mailto: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 | 2007-January-18 | 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](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. Important Notices and Privacy Statement.

---

Updated: May 14, 2007

Document ID: 81583

---