

Cisco Security Response: Rootkits on Cisco IOS Devices

<http://www.cisco.com/warp/public/707/cisco-sr-20080516-rootkits.shtml>

Revision 2.3

Last Updated 2009 November 12 1900 UTC (GMT)

For Public Release 2008 May 16 0400 UTC (GMT)

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

Contents

[Cisco Response](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)

Cisco Response

This is the Cisco PSIRT response to an issue that was disclosed by Mr. Sebastian Muniz of Core Security Technologies at the EUsecWest security conference on May 22, 2008.

No new vulnerability on the Cisco IOS software was disclosed during the presentation. To the best of our knowledge, no exploit code has been made publicly available, and Cisco has not received any customer reports of exploitation.

Cisco has analyzed the available information and recommends following industry best-practices to improve the security of all network devices. Specific recommendations are available in the Additional Information section of this Security Response.

Cisco PSIRT greatly appreciates the opportunity to work with researchers on security vulnerabilities and welcomes the opportunity to review and assist in product reports. We would like to thank Mr. Sebastian Muniz and Core Security Technologies for working with us towards the goal of keeping Cisco networks and the Internet, as a whole, secure.

Additional Information

The security of Cisco IOS devices consists of multiple factors, including physical and logical access to the device, configuration of the device, and the inherent security of the software being used. The security configuration of a device, specifically in relation to device security, is conveyed using documented best practices. The document entitled "Cisco Guide to Harden Cisco IOS Devices" (available at http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml), represents one collection of those best practices.

The integrity of the software used on Cisco IOS devices, in this case Cisco IOS software, is also important to device security. Depending on severity, security issues in Cisco IOS software are communicated to customers using Security Advisories, Security Responses, or Cisco bug release notes. Further details are documented in the Cisco Security Vulnerability Policy, available at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html.

It is possible that an attacker could insert malicious code into a Cisco IOS software image and load it onto a Cisco device that supports that image. This attack scenario could occur on any device that uses a form of software, given a proper set of circumstances. This Security Response will describe best practices that network administrators can use to reduce the risk that malicious code is installed on Cisco IOS devices. Additionally, this response will offer some methods that administrators can use to mitigate the risks of introducing malicious code into the network.

Security Best Practices

Cisco recommends that the following security best practices be implemented to improve the security posture of the network. These practices are particularly relevant to ensure that Cisco IOS devices only use authorized and unaltered Cisco IOS software images.

Supply Chain Integrity

To minimize the risk associated with malicious code, it is important that network administrators develop and consistently apply a secure methodology for Cisco IOS software image management. This secure process must be used from the time a Cisco IOS software image is downloaded from cisco.com until a Cisco IOS device begins using it.

Although processes may vary based on the network and its security and change management requirements, the following procedure represents an example of best practices that may help minimize the possibility of malicious code installation.

- When downloading a Cisco IOS software image from www.cisco.com, record the MD5 hash as presented by the Cisco IOS Upgrade Planner tool.
- Once the image has been downloaded to an administrative workstation, the MD5 hash of the local file should be verified against the hash presented by the Cisco IOS Upgrade Planner.
- Once the Cisco IOS software image file has been verified as authentic and unaltered, copy it to write-once media or media that can be rendered as read-only after the image has been written.
- Verify the MD5 hash of the file written to the read-only media to detect corruption during the copy process.
- Remove the local file on the administrative workstation.
- Relocate the read-only media to the file server that is used for Cisco IOS software image

distribution to Cisco IOS devices.

- Transfer the Cisco IOS software image from the file server to the Cisco IOS device using a secure protocol that provides both authentication and encryption.
- Verify the MD5 hash of the Cisco IOS software image on the Cisco IOS device using the procedures detailed in the 'Image File Information Using IOS Upgrade Planner' section.
- Modify the configuration of the Cisco IOS device to load the new Cisco IOS software image upon startup.
- Reload the Cisco IOS device to place the new software into service.

Implement Change Control

Change control is a mechanism through which changes being made to network devices are requested, approved, implemented, and audited. In the context of ensuring the authenticity of Cisco IOS software images used in the network, change control is relevant because it helps greatly when determining which changes have been authorized and which are unauthorized. Change control is important to help ensure that only authorized and unaltered Cisco IOS software is used on Cisco IOS devices in the network.

Harden the Software Distribution Server

The server that is used to distribute software to Cisco IOS devices in the network is a critical component of network security. Several best practices should be implemented to help ensure the authenticity and integrity of software that is distributed from this server. These best practices include:

- Application of well established operating system hardening procedures that is specific to the operating system in use
- Configuration of all appropriate logging and auditing capabilities, including logging to write-once media
- Placement of the software distribution server on a secure network with restricted connectivity from all but the most trusted networks
- The use of restrictive security controls to limit interactive access (as an example, SSH) to only a subset of trusted network administrators

Utilize Up-to-Date Software

Cisco IOS software used in the network must be kept up-to-date so that new security functionality can be leveraged and exposure to known vulnerabilities disclosed through Cisco Security Advisories is minimal.

Cisco is continually evolving the security of Cisco IOS software images through the implementation of new security functionality and the resolution of bugs. For these reasons, it is imperative that network administrators maintain their networks in a manner that includes using up-to-date software. Failure to do so could expose vulnerabilities that may be used to gain unauthorized access to a Cisco IOS device.

Leverage Authentication, Authorization, and Accounting

The comprehensive implementation of Authentication, Authorization, and Accounting (AAA) is critical to ensuring the security of interactive access to network devices. Furthermore, AAA, and specifically authorization and accounting functions, should be used to limit the actions authenticated users can perform in addition to providing an audit trail of individual user actions.

For additional information on the implementation of AAA please see the the section entitled "Using Authentication, Authorization and Accounting" (available at http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml#usingaa of the "Cisco Guide to Harden Cisco IOS Devices".

Limit Interactive Access to Devices

Once AAA has been implemented to control which users can log in to particular network devices, access control should be implemented to limit from which IP addresses users may perform management functions on a network device. This access control includes multiple security features and solutions to limit access to a device:

- VTY access classes
- Management Plane Protection (MPP)
- Control Plane Policing (CoPP)
- Control Plane Protection (CPPr)
- Infrastructure Access Control Lists (iACL)
- Simple Network Management Protocol (SNMP) access lists

For more information, please consult the following sections of the "Cisco Guide to Harden Cisco IOS devices": "Securing Interactive Management Sessions" (available at http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml#interact) and "Fortifying the Simple Network Management Protocol" (available at http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml#fortify)

Leverage Centralized and Comprehensive Logging

For network administrators to understand events taking place on a network, a comprehensive logging structure using centralized log collection and correlation must be implemented. Additionally, a standardized logging and time configuration must be deployed on all network devices to facilitate accurate logging. Furthermore, logging from the AAA functions in the network should be included in the centralized logging implementation.

Once comprehensive logging is in place on a network, the collected data must be used to monitor network activity for events that may indicate unauthorized access to a network device, or unauthorized actions by legitimate users. These types of events could represent the first step in undermining the security on a Cisco IOS device. Because the items below may represent unauthorized access or unauthorized actions, they should be monitored closely:

- The transmission of Cisco IOS software images to a Cisco IOS device using the **copy** command or local SCP, TFTP, or FTP server functionality.
- The attempted execution of certain high risk EXEC commands. The **copy**, **gdb** and **telsh** commands are some examples of commands that should be monitored. This list is not exhaustive.
- Modification of the boot environment in use on the network devices. This specifically includes the **boot** and **config-register** global configuration commands.
- Modification of the security configuration for a Cisco IOS device. This may include the removal of VTY access classes or the logging configuration or the addition of new administrative users.
- Logging related to the insertion or removal of storage media, such as flash devices.
- SNMP-related logging of attempts to modify the Cisco IOS device configuration or perform file management tasks.

- The planned and unplanned reload of the Cisco IOS software due to a software crash or the use of the **reload** command.

For more information, see the sections entitled "Centralize Log Collection and Monitoring" (available at http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml#log) and "Logging Best Practices" (available at http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml#logbest) of the "Cisco Guide to Harden Cisco IOS Devices".

Cisco IOS Image File Verification

Network administrators can use one of several security features to verify the authenticity and integrity of Cisco IOS software images in use on their network devices. It is also possible to use a process that does not rely on features in the Cisco IOS software itself.

The following sections contain information on Cisco IOS software features and administrative processes that can be used to verify the authenticity and integrity of a Cisco IOS software image.

Using the MD5 File Validation Feature

The MD5 File Validation feature, added in Cisco IOS Software Releases 12.2(4)T and 12.0(22)S, allows network administrators to calculate the MD5 hash of a Cisco IOS software image file that is loaded on a device. It also allows administrators to verify the calculated MD5 hash against that provided by the user. Once the MD5 hash value of the installed Cisco IOS image is determined, it can also be compared with the MD5 hash provided by Cisco to verify integrity of the image file.

Note: The MD5 File Validation feature can only be used to check the integrity of a Cisco IOS software image that is stored on a Cisco IOS device. It cannot be used to check the integrity of an image running in memory.

MD5 hash calculation and verification using the MD5 File Validation feature can be accomplished using the following command:

```
verify /md5 filesystem:filename [md5-hash]
```

Network administrators can use the **verify /md5** privileged EXEC command to verify the integrity of image files that are stored on the Cisco IOS file system of a device. The following shows how to use the **verify /md5** command on a Cisco IOS device:

```
router#verify /md5 disk0:c7301-jk9s-mz.124-10.bin
.....<output truncated>.....Done!
verify /md5 (disk0:c7301-jk9s-mz.124-10.bin) = ad9f9c902fa34b90de8365c3a5039a5b
router#
```

Network administrators can also provide an MD5 hash to the **verify** command. If provided, the **verify** command will compare the calculated and provided MD5 hashes as illustrated in the following example:

```
router#verify /md5 disk0:c7301-jk9s-mz.124-10.bin ad9f9c902fa34b90de8365c3a5039
.....<output truncated>.....Done!
Verified (disk0:c7301-jk9s-mz.124-10.bin) = ad9f9c902fa34b90de8365c3a5039a5b
```

```
router#
```

If the network administrator provides an MD5 hash that does not match the hash calculated by the MD5 File Validation feature, an error message will be displayed. This is illustrated in the following example:

```
router#verify /md5 disk0:c7301-jk9s-mz.124-10.bin 0c5be63c4e339707efb7881fde7d5
.....<output truncated>.....Done!

%Error verifying disk0:c7301-jk9s-mz.124-10.bin
Computed signature = ad9f9c902fa34b90de8365c3a5039a5b
Submitted signature = 0c5be63c4e339707efb7881fde7d5324

router#
```

In the preceding examples, the **verify /md5** command calculates and displays the MD5 hash for the entire Cisco IOS image file. This approach is in contrast to the updated **verify** command present with the "Image Verification" feature, which calculates the hash for the entire Cisco IOS image as well as specific portions of the uncompressed Cisco IOS image file.

For additional information on how to use this feature, please consult the document entitled "MD5 File Validation", which is available at

http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_md5_ps6350_TSD_Products_Configuration_Guide_Chapter.html.

Using the Image Verification Feature

The Image Verification feature, added in Cisco IOS Software Releases 12.3(4)T, 12.0(26)S, and 12.2(18)S, builds on the MD5 File Validation functionality to more easily allow network administrators to verify the integrity of an image file that is loaded on the Cisco IOS file system of a device. The purpose of the Image Verification feature is to ensure that corruption of the Cisco IOS software image file has not occurred. The corruption detected by this feature could have occurred at any time; for example, during the download from Cisco.com or the installation process.

Note: The Image Verification feature does not check the integrity of the image running in memory.

Cisco IOS software image file verification using this feature can be accomplished using the following commands:

- **file verify auto**
- **copy** [/erase] [/verify | /noverify] *source-url destination-url*
- **reload** [warm] [/verify | /noverify] [*text* | **in time** [*text*] | **at time** [*text*] | **cancel**]

Note: Only the **file verify auto** global configuration command and the **verify** privileged EXEC command will be covered in this Security Response. For information on the **copy /verify** and **reload /verify** commands, please see the section entitled "Image Verification" (available at http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_image_verifctn_external_docbas of the "Cisco IOS Security Configuration Guide" (available at http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.html).

Configuring the file verify auto Command

Network administrators can use the **file verify auto** global configuration command to enable verification of all images that are either copied using the **copy** privileged EXEC command or loaded using the **reload** privileged EXEC command. These images are automatically verified for image file integrity.

The following example shows how to configure the **file verify auto** Cisco IOS feature:

```
router#configure terminal
router(config)#file verify auto
router(config)#exit
router#
```

In addition to **file verify auto**, both the **copy** and the **reload** commands have a **/verify** argument that enables the Image Verification feature to check the integrity of the Cisco IOS image file. This argument must be used each time an image is copied to or reloaded on a Cisco IOS device if the global configuration command **file verify auto** is not present.

Using the Image Verification Cisco IOS verify Command

Network administrators can also use the **verify** privileged EXEC command, originally introduced for the "MD5 File Validation" feature and updated by the "Image Verification" feature, to verify the integrity of image files that are stored locally on a device. The following example demonstrates how to use the updated **verify** command on a Cisco IOS device:

```
router#verify disk0:c7301-jk9s-mz.124-10.bin
Verifying file integrity of disk0:c7301-jk9s-mz.124-10.bin
.....<output truncated>.....Done!
Embedded Hash MD5 : 0C5BE63C4E339707EFB7881FDE7D5324
Computed Hash MD5 : 0C5BE63C4E339707EFB7881FDE7D5324
CCO Hash MD5 : AD9F9C902FA34B90DE8365C3A5039A5B

Signature Verified

router#
```

In the preceding output, three MD5 hash values are displayed by the **verify** command. Here is an explanation of what each one of those MD5 hash values means:

- **Embedded Hash:** MD5 hash stored by Cisco in a section of the Cisco IOS image file during the image build process; used to verify section integrity for the Cisco IOS software image file. This MD5 hash value is calculated for certain sections of the Cisco IOS image file.
- **Computed Hash:** MD5 hash that the "Image Verification" feature calculates for certain sections of the Cisco IOS software image file when the **verify** command is executed. This value should be the same as the Embedded Hash to verify section integrity of the Cisco IOS image file. If this value is not equal to the Embedded Hash, the Cisco IOS image file may be corrupted or intentionally altered.
- **CCO Hash:** MD5 hash for the entire Cisco IOS image file. This hash is computed by the **verify** command and is not stored in the Cisco IOS software image.

For additional information please see the section entitled "Image Verification" (available at http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_image_verifctn_external.docbas of the "Cisco IOS Security Configuration Guide" (available at http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_4/sec_12_4_book.html).

Downloading an Image File From a Cisco IOS Device

In certain circumstances, network administrators may consider moving an existing Cisco IOS software image file from a Cisco IOS device to an administrative workstation. Once on the administrative workstation, independent tools can be used to calculate the MD5 hash of the file.

Two options are available for administrators to perform this task. One option allows the administrator to use the Cisco IOS software in use on the device to copy the stored Cisco IOS software image file to an administrative workstation. If this process is being carried out for security reasons, administrators are advised to use a secure protocol (such as SCP) to transfer the file. However, it is technically possible to perform this process using other protocols, including RCP, TFTP, FTP, HTTP or HTTPS. This process is accomplished using the **copy** command as illustrated in the following example:

```
router#copy flash:c7301-jk9s-mz.124-10.bin scp:c7301-jk9s-mz.124-10.bin
Address or name of remote host []? 10.1.1.1
Destination username [cisco]? user
Destination filename [c7301-jk9s-mz.124-10.bin]? <enter>
Writing c7301-jk9s-mz.124-10.bin
Password: <enter password>
! Sink: C0644 28905508 c7301-jk9s-mz.124-10.bin
!!!!<output truncated>!!!!
28905508 bytes copied in 22.280 secs (1297375 bytes/sec)
router#
```

A second and recommended option, one that provides an additional level of security, is to restart a Cisco IOS device using a known-good version of Cisco IOS software from a trusted location. Administrators can accomplish this task using the **boot system** global configuration command as illustrated in the following example:

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#boot system ftp c7301-jk9s-mz.124-10.bin 10.1.1.1
router(config)#end
router#copy running-config startup-config
Destination filename [startup-config]? <enter>

Building configuration...
[OK]
router#reload
```

Once the network device has been restarted with a known-good Cisco IOS image, a network administrator can verify the locally stored image using the **verify** command or by copying the Cisco IOS software image to a remote file server for offline verification.

Offline Image File Verification

Once a file is stored on an administrative workstation, a network administrator can verify the MD5 hash for that Cisco IOS image file using an MD5 hashing utility. Such utilities include **md5sum** for the Linux operating system, **md5** for the BSD operating system, and **fsutil**, **MD5summer**, and **WinMD5** for Microsoft Windows platforms. Additionally, the size of the Cisco IOS image file can be obtained using the **ls** command on Linux and BSD operating systems and the **dir** command on Microsoft Windows platforms.

The following example demonstrates the MD5 calculation and file size display for Linux-based systems:

```
$
$ md5sum c7301-jk9s-mz.124-10.bin
ad9f9c902fa34b90de8365c3a5039a5b c7301-jk9s-mz.124-10.bin
$
$ ls -l c7301-jk9s-mz.124-10.bin
-r--r--r--  1 user user 28905508 May 16 15:17 c7301-jk9s-mz.124-10.bin
$
```

The following example illustrates this process for BSD-derived systems:

```
$
$ md5 c7301-jk9s-mz.124-10.bin
MD5 (c7301-jk9s-mz.124-10.bin) = ad9f9c902fa34b90de8365c3a5039a5b
$
$ ls -l c7301-jk9s-mz.124-10.bin
-r--r--r--  1 user  user 28905508 May 16 21:36 c7301-jk9s-mz.124-10.bin
$
```

The following example shows the use of the **fsum** utility and the **dir** command on a Windows system:

```
C:\>fsum -md5 c7301-jk9s-mz.124-10.bin

SlavaSoft Optimizing Checksum Utility - fsum 2.52.00337
Implemented using SlavaSoft QuickHash Library <www.slavasoft.com>
Copyright (C) SlavaSoft Inc. 1999-2007. All rights reserved.

; SlavaSoft Optimizing Checksum Utility - fsum 2.52.00337 <www.slavasoft.com>
;
; Generated on 05/20/08 at 00:01:13
;
ad9f9c902fa34b90de8365c3a5039a5b *c7301-jk9s-mz.124-10.bin

C:\>
C:\>dir c7301-jk9s-mz.124-10.bin
Directory of C:\

05/20/2008  00:10 AM           28,905,508 c7301-jk9s-mz.124-10.bin
                1 File(s)          28,905,508 bytes

                0 Dir(s)      1,207,291,904 bytes free

C:\>
```

Note: The use of the **fsum** utility is for illustrative purposes only and should not be interpreted as an endorsement of the tool.

Image File Information Using Cisco IOS Upgrade Planner

Once the MD5 hash and file size for a Cisco IOS software image has been collected, network administrators can verify authenticity of the image using information provided by the Cisco IOS Upgrade Planner tool during the download process. The Cisco IOS Upgrade Planner tool requires a valid Cisco.com account and provides details about each publicly available IOS image.

Network administrators must identify their Cisco IOS software release (this can be done by using information obtained from output provided by the **show version** command) and navigate through the Cisco IOS Upgrade Planner tool to locate the image in use on the Cisco IOS device. Network administrators should verify that the CCO Hash calculated by the Cisco IOS **verify** command (part of the Cisco IOS "Image Verification" feature), the MD5 hash calculated by the **verify /md5** command (part of the "MD5 File Validation" Cisco IOS feature), or the MD5 hash calculated by a third-party utility matches the MD5 hash that is provided by the Cisco IOS Upgrade Planner tool.

If the MD5 hash value for the whole Cisco IOS image file does not match the MD5 hash provided by Cisco, network administrators should download the Cisco IOS image file from the Cisco IOS Upgrade Planner and use the file verification methods described in this document to verify integrity of the Cisco IOS image file.

The following is an example of the information provided by the Cisco IOS Upgrade Planner tool during one of the steps required for downloading a Cisco IOS software image file from www.cisco.com:

Details	Example
Release	12.4.10
Size	28905508
BSD Checksum	47318
Router Checksum	0x3b61
MD5	ad9f9c902fa34b90de8365c3a5039a5b
Date Published	17-AUG-2006

For those customers whose www.cisco.com account does not provide access to the Cisco IOS Upgrade Planner tool and hence cannot obtain the Cisco calculated, known-good MD5 hash value for a given Cisco IOS software image, or for those customers that would prefer to automate the process of validating MD5 hashes using their own tools, Cisco is making available a compressed file including the Cisco IOS software image name and known-good MD5 hash for all 12.0-based, 12.1-based, 12.2-based, 12.3-based, 12.4-based and 15.0-based Cisco IOS software releases.

This file can be found at <http://www.cisco.com/web/tsweb/psirt/cisco-sr-20080516-rootkits-r2.3.zip> and contains a second compressed file (a set of data files and a document explaining the file format) and a detached PGP signature for the second compressed file. The file has been signed by the current Cisco PSIRT PGP key. Information on how to obtain the current Cisco PSIRT PGP key can be found in the document entitled "Cisco Security Vulnerability Policy", available at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html.

We recommend customers to uncompress the file and verify the signature for the second file before using the data files for any verification purposes.

Revision History

Revision 2.3	2009- November-12	Updated Cisco IOS hashes file

Revision 2.2	2009-August-07	Fixed broken links
Revision 2.1	2008-June-23	Fixed broken links
Revision 2.0	2008-May-22	Updated Additional Information section with best practices content
Revision 1.0	2008-May-16	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>.

Help us help you.

Please rate this document.

- Excellent
 Good
 Average
 Fair
 Poor

This document solved my problem.

- Yes
 No
 Just browsing

Suggestions for improvement:

(256 character limit)

Send

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 - 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)