

Cisco Security Advisory: Multiple Vulnerabilities in the IOS FTP Server

Advisory ID: cisco-sa-20070509-iosftp

<http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml>

Revision 1.3

Last Updated 2008 May 14 2000 UTC (GMT)

For Public Release 2007 May 09 1600 UTC (GMT)

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

Contents

- [Summary](#)
- [Affected Products](#)
- [Details](#)
- [Vulnerability Scoring 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 IOS FTP Server feature contains multiple vulnerabilities that can result in a denial of service (DoS) condition, improper verification of user credentials, and the ability to retrieve or write any file from the device filesystem, including the device's saved configuration. This configuration file may include passwords or other sensitive information.

The IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS FTP Server service are unaffected by these vulnerabilities.

This vulnerability does not apply to the IOS FTP Client feature.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ **Affected Products**

☐ **Vulnerable Products**

Cisco devices running IOS and configured for FTP server functionality are affected by these issues.

IOS versions based on 11.3, 12.0, 12.1, 12.2, 12.3 and 12.4 contain the IOS FTP server feature. The IOS FTP server feature was removed via CSCsg16908.

Only certain IOS releases based on the above IOS trains contain the IOS FTP server feature. For a device running Cisco IOS to be vulnerable, the following command must be present in the device configuration:

```
ftp-server enable
```

☐ **Products Confirmed Not Vulnerable**

Cisco devices that do not run IOS are not affected.

Cisco IOS devices that do not have the FTP server feature enabled are not affected.

Cisco IOS XR is not affected.

No other Cisco devices are known to be affected.

[Top of the section](#) [Close Section](#)

☐ **Details**

Multiple vulnerabilities exist in the IOS FTP Server feature. These vulnerabilities are documented with the following Cisco bug IDs:

- CSCek55259 - Improper authorization checking in IOS FTP server
- CSCse29244 - IOS reload when transferring files via FTP

Due to these issues with the IOS FTP server, the feature is being removed. Cisco is considering adding fully featured and secure FTP server functionality at a later date.

The IOS FTP Server feature removal is addressed with Cisco bug ID CSCsg16908.

[Top of the section](#) [Close Section](#)

▣ 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>.

CSCek55259 - Improper authorization checking in IOS FTP						
Calculate the environmental score of CSCek55259						
CVSS Base Score - 10						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	Complete	Complete	Complete	Normal
CVSS Temporal Score - 8.3						
Exploitability		Remediation Level		Report Confidence		
Functional		Official-Fix		Confirmed		

CSCse29244 - IOS reload when transferring files via FTP						
Calculate the environmental score of CSCse29244						
CVSS Base Score - 2.0						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Required	None	None	Complete	Normal
CVSS Temporal Score - 1.7						

Exploitability	Remediation Level	Report Confidence
Functional	Official-Fix	Confirmed

[Top of the section](#) [Close Section](#)

☐ Impact

Successful exploitation of these vulnerabilities may allow unauthorized, remote users to access the filesystem on the IOS device, cause the affected device to reload, or execute arbitrary code.

Unauthorized users could retrieve the device's startup-config file from the filesystem. This file may contain information that could allow the attacker to gain escalated privileges.

Repeated exploitation of the vulnerabilities could lead to an extended Denial of Service (DoS).

[Top of the section](#) [Close Section](#)

☐ 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.

Each row of the Cisco IOS software table (below) describes a release train. If a given release train is vulnerable, then the earliest possible releases that contain the fix (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Rebuild" and "Maintenance" columns. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

Software releases that are not listed in the below table are not affected.

For more information on the terms "Rebuild" and "Maintenance," consult the following URL: <http://www.cisco.com/warp/public/620/1.html>.

Major Release	Availability of Repaired Releases	
	Rebuild	Maintenance
Affected 12.0-Based Release		
12.0	Vulnerable; migrate to 12.2(40a) or later	
	Vulnerable; migrate to 12.2(40a)	

12.0T	or later	
12.0XC	Vulnerable; migrate to 12.2(40a) or later	
12.0XK	Vulnerable; migrate to 12.2(40a) or later	
12.0WC	12.0(5)WC17	
Affected 12.1-Based Release	Rebuild	Maintenance
12.1	Vulnerable; migrate to 12.2(40a) or later	
12.1T	Vulnerable; migrate to 12.2(40a) or later	
12.1XH	Vulnerable; migrate to 12.2(40a) or later	
12.1XM	Vulnerable; migrate to 12.3(21) or later	
Affected 12.2-Based Release	Rebuild	Maintenance
12.2	12.2(40a)	12.2(46)
12.2T	Vulnerable; migrate to 12.3(21) or later	
12.2XA	Vulnerable; migrate to 12.3(21) or later	
12.2XG	Vulnerable; migrate to 12.3(21) or later	
12.2XT	Vulnerable; migrate to 12.3(21) or later	
12.2ZF	Vulnerable; migrate to 12.4(12) or later	
12.2ZH	Vulnerable; contact TAC	
12.2ZJ	Vulnerable; migrate to 12.4(12) or later	
12.2ZL	Vulnerable; contact TAC	
12.2ZN	Vulnerable; migrate to 12.4(12) or later	
Affected 12.3-Based Release	Rebuild	Maintenance
12.3		12.3(21)
12.3B	Vulnerable; migrate to 12.4(12) or	

	later
12.3T	Vulnerable; migrate to 12.4(12) or later
12.3TPC	Vulnerable; contact TAC
12.3XA	Vulnerable; contact TAC
12.3XC	Vulnerable; contact TAC
12.3XD	Vulnerable; migrate to 12.4(12) or later
12.3XE	Vulnerable; contact TAC
12.3XF	Vulnerable; migrate to 12.4(12) or later
12.3XG	Vulnerable; contact TAC
12.3XH	Vulnerable; migrate to 12.4(12) or later
12.3XK	Vulnerable; migrate to 12.4(12) or later
12.3XQ	Vulnerable; migrate to 12.4(12) or later
12.3XR	Vulnerable; contact TAC
12.3XS	Vulnerable; migrate to 12.4(12) or later
12.3XX	12.3(8)XX2d
12.3YA	Vulnerable; migrate to 12.4(12) or later
12.3YD	Vulnerable; migrate to 12.4(11)T or later
12.3YG	Vulnerable; migrate to 12.4(11)T or later
12.3YH	Vulnerable; migrate to 12.4(11)T or later
12.3YI	Vulnerable; migrate to 12.4(11)T or later
12.3YK	Vulnerable; migrate to 12.4(11)T or later
12.3YM	Vulnerable; contact TAC
12.3YS	Vulnerable; migrate to 12.4(11)T or later
12.3YT	Vulnerable; migrate to 12.4(11)T or later

12.3YZ	Vulnerable; contact TAC	
Affected 12.4-Based Release	Rebuild	Maintenance
12.4	12.4(10b)	
	12.4(3g)	
	12.4(7d)	
	12.4(8c)	12.4(12)
12.4SW	Vulnerable; contact TAC	
12.4T	12.4(4)T6	
	12.4(6)T6	
	12.4(9)T2	12.4(11)T
12.4XA	Vulnerable; migrate to 12.4(6)T6 or later	
12.4XC	12.4(4)XC6	
12.4XD	12.4(4)XD4	
12.4XE	12.4(6)XE2	

[Top of the section](#) [Close Section](#)

☐ Workarounds

Customers can disable the use of the IOS FTP Server feature by executing the following command in configuration mode:

```
no ftp-server enable
```

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Mitigation Bulletin companion document for this advisory:

<http://www.cisco.com/warp/public/707/cisco-amb-20070509-iosftp.shtml>

Alternative File Transfer Mechanisms

Cisco IOS supports multiple methods for transferring files to and from the device. One such method is Secure Copy (SCP). SCP is supported on Cisco IOS images that support strong cryptography. More information on the SCP feature can be found at the following url:

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a008048

Another alternative is using the Trivial File Transfer Protocol (TFTP) server in IOS. Information on configuring the TFTP server can be found here:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09

If disabling the IOS FTP Server is not feasible, customers can limit FTP access to the device via one of the following mechanisms:

Infrastructure ACLs (iACL)

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability. The ACL example shown below should be included as part of the deployed infrastructure access-list which will protect all devices with IP addresses in the infrastructure IP address range.

A sample access list for devices running Cisco IOS is below:

```
!--- Permit FTP services from trusted hosts destined
!--- to infrastructure addresses.

access-list 150 permit tcp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK
access-list 150 permit tcp TRUSTED_HOSTS MASK INFRASTRUCTURE_ADDRESSES MASK

!--- Deny FTP packets from all other sources destined to infrastructure addr

access-list 150 deny tcp any INFRASTRUCTURE_ADDRESSES MASK eq 21
access-list 150 deny tcp any INFRASTRUCTURE_ADDRESSES MASK eq 20

!--- Permit all other traffic to transit the device.

access-list 150 permit IP any any

interface serial 2/0
 ip access-group 150 in
```

The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection access lists. This white paper can be obtained here: <http://www.cisco.com/warp/public/707/iacl.html>.

Receive ACLs (rACL)

For distributed platforms, Receive ACLs may be an option starting in Cisco IOS Software Versions 12.0(21)S2 for the 12000 (GSR), 12.0(24)S for the 7500, and 12.0(31)S for the 10720. The Receive ACL protects the device from harmful traffic before the traffic can impact the route processor. Receive ACLs are designed to only protect the device on which it is configured. On the 12000, 7500, and 10720, transit traffic is never affected by a receive ACL. Because of this, the destination IP address "any" used in the example ACL entries below only refer to the router's own physical or virtual IP addresses. Receive ACLs are considered a network security best practice, and should be

considered as a long-term addition to good network security, as well as a workaround for this specific vulnerability. The white paper entitled "GSR: Receive Access Control Lists" will help you identify and allow legitimate traffic to your device and deny all unwanted packets: <http://www.cisco.com/warp/public/707/racl.html>.

The following is the receive path ACL written to permit this type of traffic from trusted hosts:

```
!--- Permit FTP from trusted hosts allowed to the RP.

access-list 151 permit tcp TRUSTED_ADDRESSES MASK any eq 21
access-list 151 permit tcp TRUSTED_ADDRESSES MASK any eq 20

!--- Deny FTP from all other sources to the RP.

access-list 151 deny    tcp any any eq 21
access-list 151 deny    tcp any any eq 20

!--- Permit all other traffic to the RP.
!--- according to security policy and configurations.

access-list 151 permit ip any any

!--- Apply this access list to the 'receive' path.

ip receive access-list 151
```

Control Plane Policing (CoPP)

The Control Plane Policing (CoPP) feature may be used to mitigate these vulnerabilities. In the following example, only FTP traffic from trusted hosts and with 'receive' destination IP addresses is permitted to reach the route processor (RP).

It should be noted that dropping traffic from unknown or untrusted IP addresses may affect hosts with dynamically assigned IP addresses from connecting to the Cisco IOS device.

```
access-list 152 deny    tcp TRUSTED_ADDRESSES MASK any eq 21
access-list 152 deny    tcp TRUSTED_ADDRESSES MASK any eq 20
access-list 152 permit tcp any any eq 20
access-list 152 permit tcp any any eq 21
access-list 152 deny    ip any any
!
class-map match-all COPP-KNOWN-UNDESIRABLE
  match access-group 152
!
!
policy-map COPP-INPUT-POLICY
  class COPP-KNOWN-UNDESIRABLE
    drop
```

```
!  
control-plane  
service-policy input COPP-INPUT-POLICY
```

In the above CoPP example, the ACL entries that match the exploit packets with the "permit" action result in these packets being discarded by the policy-map "drop" function, while packets that match the "deny" action are not affected by the policy-map drop function.

CoPP is available in Cisco IOS release trains 12.0S, 12.2SX, 12.2S, 12.3T, 12.4, and 12.4T.

Additional information on the configuration and use of the CoPP feature can be found at the following URL:

http://www.cisco.com/en/US/products/ps6642/products_white_paper0900aecd804fa16a.shtml

[Top of the section](#) [Close Section](#)

☐ **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.

[Top of the section](#) [Close Section](#)

☐ **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>.

[Top of the section](#) [Close Section](#)

☐ **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.

[Top of the section](#) [Close Section](#)

☐ **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.

[Top of the section](#) [Close Section](#)

☐ **Exploitation and Public Announcements**

The Cisco PSIRT is not aware of malicious use of the vulnerability described in this advisory. Andy Davis has published exploit code for this vulnerability.

[Top of the section](#) [Close Section](#)

☐ **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-20070509-iosftp.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 1.3	2008-May-14	Updates to the Workarounds > Receive ACLs section.
Revision 1.2	2008-April-25	Updated links to the CVSS scoring for CSCek55259 and CSCse29244 .
Revision 1.1	2007-May-09	Minor grammatical and style edits
Revision 1.0	2007-May-09	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