

# Cisco Security Advisory: TFTP Long Filename Vulnerability

Document ID: 25889

Advisory ID: cisco-sa-20020730-ioc-tftp-lfn

<http://www.cisco.com/warp/public/707/cisco-sa-20020730-ioc-tftp-lfn.shtml>

## Revision 1.3

Last Updated 2003 August 20 1800 UTC (GMT)

For Public Release 2002 July 30 1800 UTC (GMT)

---

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

---

[Summary](#)

[Affected Products](#)

[Details](#)

[Impact](#)

[Software Versions and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of This Notice: FINAL](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

---

## Summary

Trivial File Transfer Protocol (TFTP) is a protocol which allows for easy transfer of files between network connected devices. A vulnerability has been discovered in the processing of filenames within a TFTP read request on IOS devices and PXM-1 based MGX switches.

The following products are identified as affected by this vulnerability:

- MGX 8230, 8250 and PXM-1 based MGX 8850 switches running versions 1.2.10 or below
- Cisco IOS devices running versions 11.1, 11.2, 11.3

Unless explicitly stated otherwise, all other Cisco products are not affected.

There is no workaround on MGX switches.

On IOS devices, a simple workaround exists, which is detailed in the [Workarounds](#) section below.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20020730-ioc-tftp-lfn.shtml>.

# Affected Products

This section provides details on affected products.

## Vulnerable Products

The following products are affected:

- MGX 8230, 8250 and PXM-1 based MGX 8850 switches running versions 1.2.10 or below
- Cisco IOS devices running versions 11.1, 11.2, 11.3

## Products Confirmed Not Vulnerable

The following products are not affected:

- MGX 8830 switches
- MGX 8850 switches that are not PXM-1 based
- Cisco IOS software versions 11.1, 11.2, 11.3 when running on a 68040 based architecture such as a Route Processor.

Only this specific architecture is not vulnerable to a reload with the above generally affected versions. Other devices such as Route Switch Processors are affected. To verify which type of route processor you have, issue the command **show version** at the prompt on the router and look for a string similar to:

```
cisco RP1 (68040) processor (revision A0) with 16384K bytes of memory.
```

- IOS devices running IOS software versions 12.0 and above

No other Cisco products are currently known to be affected by these vulnerabilities.

## Details

The original report is located at <http://online.securityfocus.com/archive/1/284634>. Cisco responded with the following, which is also archived at <http://online.securityfocus.com/archive/1/284688>. A researcher report can also be found at [http://www.phenoelit.de/stuff/Cisco\\_tftp.txt](http://www.phenoelit.de/stuff/Cisco_tftp.txt).

By sending a crafted TFTP read request it is possible to trigger a buffer overflow in the TFTP server. On IOS devices this can only happen if no alias for all files being served has been defined.

This vulnerability can be exploited remotely.

On MGX switches, a successful exploitation will suspend the tftp service, but the switch will continue working.

On IOS devices, a successful exploitation may cause a software reset of device.

This vulnerability has been documented as CSCdy22809 for MGX switches and CSCdy03429 for IOS.

## Impact

Successful exploitation of this vulnerability on MGX switches may suspend the tftp service but the switch will continue working. The tftp service can be recovered by reloading the switch.

Successful exploitation of this vulnerability on IOS devices may cause a software reset of the device resulting in a loss of availability while the device reinitializes. Repeated exploitations could result in a Denial of Service until the workarounds for this vulnerability have been implemented.

## Software Versions and Fixes

This problem is fixed in the 1.2.11 version of WAN switching software for MGX switches.

The affected IOS releases, 11.1, 11.2, and 11.3, are all at End of Life, which means they do not have a maintenance version scheduled, and will not be fixed. It is recommended to use the documented workarounds if these versions must be used.

## Workarounds

There is no workaround on MGX switches.

There are two workarounds on IOS devices to address this issue.

### Disable the TFTP server entirely

Cisco IOS provides TFTP server functionality to facilitate the transfer of Cisco IOS images when another TFTP server may not be available. If the TFTP server functionality is not currently needed, the following steps may be taken to disable the TFTP server.

1. While in enable mode on the router, issue the command **show running-config** and look for lines starting with **tftp-server**.
2. For each line in the config starting with **tftp-server**, prepend the word **no** followed by a space followed by the full text of the matching line in config mode to remove that entry. This step must be repeated for each matching line of the config.
3. Once this task has been completed, verify that there are no lines starting with **tftp-server** by issuing the command **show running-config** from the enable prompt.
4. Once verified, save the new configuration so that the server will be disabled upon the next reset of the device.

### Provide aliases for TFTP server filenames

Cisco IOS provides the ability to alias a long filename to a shorter filename. If the **tftp-server** entries in the configuration have the keyword "alias" in them, the router will not be vulnerable to exploitation of this vulnerability. To implement this workaround, follow the directions above for disabling the TFTP server, and then add any configuration lines back to the config by appending the keyword "alias" followed by a short filename such that the command resembles:

```
tftp-server flash rsp-jv-mz.111-24a alias CiscoIOS
```

Note that this must be done for every line starting with "tftp-server" in the configuration. The existence of a single line in the configuration beginning with "tftp-server" without an alias defined while running affected versions of software is all that is needed to become subject to this vulnerability.

## Obtaining Fixed Software

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

This vulnerability was initially reported to the Cisco PSIRT by Phenoelit and was later announced on the BUGTRAQ mailing list on 2002-07-27 (<http://online.securityfocus.com/archive/1/284634> ). Cisco responded with the message at <http://www.securityfocus.com/archive/1/284688> and this notice.

The Cisco PSIRT is not aware of any malicious use of the vulnerability described in this advisory.

## 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 notice will be posted on Cisco's Worldwide Web site at <http://www.cisco.com/warp/public/707/cisco-sa-20020730-ioc-tftp-lfn.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
- bugtraq@securityfocus.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- comp.dcom.sys.cisco
- firewalls@lists.gnac.com
- Various internal Cisco mailing lists

Future updates of this notice, if any, will be placed on Cisco's Worldwide Web server, but may or may not be actively announced on mailing lists or newsgroups.

Users concerned about this problem are encouraged to check the URL given above for any updates.

## Revision History

Revision 1.3	2003-August-20	Corrected ID number for MGX switches
Revision 1.2	2003-August-14	Added the information about MGX switches
Revision 1.1	2002-August-20	Credited vulnerability reporter in Public Announcements
Revision 1.0	2002-July-30	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 Web site 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: Aug 20, 2003

Document ID: 25889

---