

[NEWS] TFTP Long Filename Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0143.html>

From: support@securiteam.com

Date: 07/31/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 31 Jul 2002 19:55:08 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

TFTP Long Filename Vulnerability

SUMMARY

Trivial File Transfer Protocol (TFTP) is a protocol that 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 when Cisco IOS® is configured to act as a TFTP server.

The following products are identified as affected by this vulnerability:

- * Cisco IOS software versions 11.1, 11.2, 11.3

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

A simple workaround exists for the vulnerability that is detailed in the Workarounds section below.

DETAILS

Affected Products:

The following products are affected:

- * Cisco IOS software versions 11.1, 11.2, 11.3

The following products are not affected:

- * Cisco IOS software versions 11.1, 11.2, 11.3 when running on a 68040

Securiteam: [NEWS] TFTP Long Filename Vulnerability

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.

* Cisco IOS software versions 12.0 and up.

Details:

By sending a crafted TFTP read request it is possible to trigger a buffer overflow in the TFTP server when no alias for all files being served have been defined. This vulnerability can be exploited remotely. The successful exploitation may cause a software reset of the device.

This vulnerability has been documented as CSCdy03429.

Impact:

Successful exploitation of this vulnerability 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:

The affected 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.

Obtaining Fixed Software:

As the affected versions are not scheduled to be fixed, and a simple workaround is available, a software upgrade is not required to address this vulnerability. However, if you have a service contract, and wish to upgrade to unaffected code, you may obtain upgraded software through your regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's Worldwide Web site at <http://www.cisco.com> > <http://www.cisco.com>.

If you need assistance with the implementation of the workarounds, or have questions on the workarounds, please contact the Cisco Technical Assistance Center (TAC).

Cisco 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

Securiteam: [NEWS] TFTP Long Filename Vulnerability

See <<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>>
<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.

Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

Workarounds:

There are two workarounds known 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.

ADDITIONAL INFORMATION

Securiteam: [NEWS] TFTP Long Filename Vulnerability

The information has been provided by <mailto:psirt@cisco.com> Cisco Systems Product Security Incident Response Team.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[\[UNIX\] Incomplete Patch for File Descriptor Vulnerability Allows Insertion of Arbitrary Content into Sensitive Files](#)"
 - **Messages sorted by:** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)