

Cisco Security Response: Wide Area Application Services (WAAS) Common UNIX Printing System (CUPS) Vulnerability

<http://www.cisco.com/warp/public/707/cisco-sr-20080625-waas.shtml>

Revision 1.0

For Public Release 2008 June 25 1600 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 a security advisory regarding a vulnerability in Common UNIX Printing System (CUPS). The CUPS security advisory can be found at <http://www.cups.org/str.php?L2561>.

The Cisco Wide Area Application Services (WAAS) incorporates a print server based on the integration of open source CUPS technology, which is affected by this CUPS vulnerability.

This vulnerability can be remotely exploited and could result in execution of arbitrary code on the Cisco WAAS products.

Additional Information

CSCsI92095 - Missing IPP value length range checks (STR #2561)

This vulnerability is referenced by CUPS as STR #2561. This CUPS vulnerability is caused by a boundary error in the "ippReadIO()" function in cups/ipp.c when processing IPP (Internet Printing Protocol) tags. Attackers can exploit this vulnerability to overwrite one byte on the stack with a zero by sending an IPP request that contains specially crafted "textWithLanguage" or

"nameWithLanguage" tags.

The version of CUPS that is used in WAAS system software prior to version 4.0.19 is affected by this vulnerability in processing IPP tags if print services are enabled on the WAAS.

To determine the system software version in use on the WAAS use the graphical user interface (GUI) or command-line interface (CLI):

- Log in to the WAAS Central Manager GUI and choose **Devices > Devices**. The Devices window displays the software version for each device listed. Alternatively, in the contents pane for any given device, choose **Monitoring > Show/Clear Commands > Show Commands**. Choose **version** and click Submit. A secondary window pops up and displays the command line interface (CLI) output for the show version command.

- Log into the device, and use the CLI to enter the command **show version**. The following example shows output from a device that is running 4.0.17 build 14.

```

waas_lab#show version
Cisco Wide Area Application Services Software (WAAS)
Copyright (c) 1999-2008 by Cisco Systems, Inc.
Cisco Wide Area Application Services Software Release 4.0.17 (build b14 Feb
Version: oe7326-4.0.17.14

Compiled 14:42:31 Feb 27 2008 by cnbuild

System was restarted on Thu May 15 16:07:56 2008.
The system has been up for 3 days, 21 hours, 53 minutes, 26 seconds.

```

By default, the WAAS print services feature is disabled on all WAAS devices.

To determine if print services have been enabled do one of the following:

- Log in to the WAE Device Manager GUI choose **Configuration** from the WAFS Edge menu. In the **Print Services** tab there is a check box for **Print services enabled**. If this check box is marked the print services are enabled.

- Log into the device, and use the CLI to enter the command **show running-config | include print-services enable** command. If the command returns **print-services enable**, print services are enabled. The following example shows the output when print services are enabled:

```

waas_lab#show running-config | include print-services enable
print-services enable
waas_lab#

```

The following example shows the output when print services are not enabled:

```

waas_lab#show running-config | include print-services enable
waas_lab#

```

If this CUPS vulnerability is exploited, the CUPS process will crash and automatically be restarted by the system. Other WAAS functions will not be affected during any active exploitation.

Successful exploitation could also allow the execution of arbitrary code under the context of the CUPS process privilege only.

For more information about print services on the WAAS, consult the following link:

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v4013/configuration/guide/printsrv

This vulnerability is documented in Cisco bug ID [CSCsI92095](#) ([registered](#) customers only) and has been assigned Common Vulnerabilities and Exposures (CVE) Identifier CVE-2007-4351.

Software Versions and Fixes

Software versions 4.0.19.14 and later contain the fix for this vulnerability. The software is available for download from: <http://www.cisco.com/cgi-bin/tablebuild.pl/waas40?psrtdcat20e2>

Note: The End of Life Cisco Wide Area File Services Software (WAFS) is also affected by this vulnerability. The vulnerability for the WAFS is documented in Cisco bug ID [CSCsI92099](#) ([registered](#) customers only) . There are no planned software releases for the WAFS. Customers are encouraged to migrate to WAAS.

Workarounds

If the print services are not required on the WAAS, disable them. To disable print services on the WAAS do either of the following:

- Log in to the WAE Device Manager GUI and choose **Configuration** from the WAFS Edge menu. Under the **Print Services** tab there is a check box for **Print services enabled**. Ensure this check box is not marked.
- Log into the WAAS device and from the CLI prompt, enter configuration mode and enter the command **no print-services enable**.

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

<http://www.cisco.com/warp/public/707/cisco-amb-20080625-waas.shtml>

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.

Revision History

Revision 1.0	2008-June-25	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)

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

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

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)