

Cisco Security Response: Cisco IOS Reload on Regular Expression Processing

<http://www.cisco.com/warp/public/707/cisco-sr-20070912-regex.shtml>

Revision 1.2

Last Updated 2007 September 19 1800 UTC (GMT)

For Public Release 2007 September 12 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 Product Security Incident Response Team (PSIRT) response to a vulnerability that was reported on the Cisco NSP mailing list on August 17, 2007 regarding the crash and reload of devices running Cisco IOS® after executing a command that uses, either directly or indirectly, a regular expression. The original post is available at the following link:

<http://puck.nether.net/pipermail/cisco-nsp/2007-August/043002.html>

The Cisco PSIRT posted a preliminary response on the same day and is available at the following link:

<http://puck.nether.net/pipermail/cisco-nsp/2007-August/043010.html>

Preliminary research pointed to a previously known issue that was documented as Cisco bug ID [CSCsb08386](#) ([registered](#) customers only) , and entitled "PRP crash by show ip bgp regexp", which was already resolved. Further research indicates that the current issue is a different but related vulnerability.

There are no workarounds available for this vulnerability. Cisco will update this document in the event of any changes.

Additional Information

Cisco IOS includes a regular expression engine that is used to process regular expressions that are provided as part of a command that is typed on the command line interface (CLI), as seen in the following example:

```
Router#show ip bgp regexp [regexp]
```

or

When using a regular expression as part of a filter that is invoked after piping the output of a command into a filter, as seen in the following example:

```
Router#show running-config | include [regexp]
```

or

From the "--more--" prompt while paginating through the output of a previously executed command, by typing "/[regexp]" while on the "--more--" prompt.

Some regular expressions that make use of combined repetition operators ('*' or '+') and pattern recalls ("\1", "\2", etc.) into the same expression may result in a stack overflow on the Cisco IOS regular expression engine. A stack overflow will result in a reload of the device.

Note: To execute such commands including regular expressions, a user has to have access to the device CLI. This access implies that a user can log in into the device by providing valid user credentials.

Products Affected by This Vulnerability

Note: The following list is subject to change. Cisco is continuing to review the potential impact of this vulnerability on its products; this list may be updated to include additional Cisco products that are affected by this vulnerability.

- Cisco IOS releases 12.0, 12.1, 12.2, 12.3 and 12.4 - Cisco bug IDs are [CSCsk14633](#) ([registered customers only](#)) and [CSCsk33054](#) ([registered customers only](#)) .

No other Cisco products are currently known to be affected by this vulnerability. Cisco IOS XR is not affected by this vulnerability.

Workarounds

There is no workaround for this vulnerability.

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 1.2	2007-September-19	Updated links to the Cisco NSP external list archives.
Revision 1.1	2007-September-18	Changed title to better reflect affected product. Added '+' to the list of repetition operators known to cause the crash.
Revision 1.0	2007-September-12	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

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.](#)