

Table of Contents

<u>Cisco Security Notice: Sending 2GB Data in GET Request Causes Buffer Overflow in Cisco IOS Software</u>	1
<u>Revision 1.1</u>	1
<u>For Public Release 2003 July 30</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Affected Products</u>	1
<u>Fixed Software</u>	1
<u>Workarounds</u>	2
<u>Cisco Security Procedures</u>	2
<u>Related Information</u>	2

Cisco Security Notice: Sending 2GB Data in GET Request Causes Buffer Overflow in Cisco IOS Software

Revision 1.1

For Public Release 2003 July 30

Please provide your feedback on this document.

Summary
Affected Products
Fixed Software
Workarounds
Cisco Security Procedures
Related Information

Summary

If Hypertext Transfer Protocol (HTTP) server is enabled on a Cisco IOS® software device, it is vulnerable to a malformed HTTP GET request which contains two gigabytes of data. This will cause the router to reload with a buffer overflow condition. It may be exploited to execute arbitrary code on the router.

HTTP server is enabled on a Cisco IOS device if **ip http server** is present in the configuration.

Affected Products

All Cisco IOS software versions except 12.3 and 12.3T are affected. CatOS and PIX are not affected.

This vulnerability has been assigned the Cisco bug ID CSCeb50339 (registered customers only) . Workarounds are available to mitigate the effects.

This vulnerability has been discovered by FX of Phenoelit.

Fixed Software

This vulnerability is currently fixed or scheduled to be fixed in the following Cisco IOS software versions:

Train	Description	Interim	Maintenance
12.0S	Core/ISO	12.0(25.4)S1	12.0(26)S (2003–Aug)
12.1	General Deployment		12.1(22) (2003–Dec)
12.1E	Enterprise Support	12.1(19.3)E (2003–Aug–01)	12.1(20)E (2003–Sep–29)

12.2	12.2 Mainline	12.2(18.2)	12.2(19) (2003–Aug–25)
12.2T	Technology Train	12.2(15)T	12.2(15)T5
12.2JA	Access Point Special	12.2(11)JA1	12.2(11)JA1
Note: 12.3 and 12.3T–based images are not vulnerable.			

Workarounds

The workaround is to configure access lists to explicitly permit authorized hosts or networks to the http service.

The syntax for this command for routers and switches running Cisco IOS software is:

```
ip http access-class access-list number

access-list access-list number permit host authorized host #1

access-list access-list number permit host authorized host #2

.....
access-list access-list number deny any
```

The *access-list number* in the above example needs to be in the range of 1–99.

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/warp/public/707/sec_incident_response.shtml. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

Related Information

- [Cisco Product Security Advisories and Notices](#)
 - [Technical Support – Cisco Systems](#)
-

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.