

Table of Contents

<u>Cisco Security Notice: Data Leak in UDP Echo Service</u>	1
<u>Revision 1.0</u>	1
<u>For Public Release 2003 July 31</u>	1
<u>Please provide your feedback on this document</u>	1
<u>Summary</u>	1
<u>Fixed Software</u>	1
<u>Workarounds</u>	1
<u>Cisco Security Procedures</u>	2
<u>Related Information</u>	2

Cisco Security Notice: Data Leak in UDP Echo Service

Revision 1.0

For Public Release 2003 July 31

Please provide your feedback on this document.

Summary
Fixed Software
Workarounds
Cisco Security Procedures
Related Information

Summary

If the **udp-small-servers** command is enabled, a Cisco IOS® software device may reply to malformed udp echo packets with some of the contents stored in a router's memory. By repeatedly sending malformed udp echo packets and capturing the replies, an attacker can obtain portions of the data that is stored in a router's memory.

Workarounds are available to mitigate the effects.

Fixed Software

This vulnerability has been fixed by the Cisco Bug ID CSCdk77834 (registered customers only) . Below are the first Cisco IOS software releases that are not affected by this vulnerability:

- 12.0(3.2)
- 12.0(3.3)S
- 12.0(3.4)T
- 12.0(3.6)W5(9.0.5)

12.1, 12.2, and 12.3-based images are not affected.

Workarounds

The workaround is to disable **udp-small-services**. The syntax for this command on routers and switches running Cisco IOS software is as follows:

```
no service udp-small-servers
```

The **udp-small-servers** command is disabled by default since Cisco IOS Software Release 11.2(1).

It is always recommended to disable unnecessary services on routers and switches. Refer to Improving Security on Cisco Routers for more information on improving router security.

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.