

Cisco Security Notice: Response to BugTraq – Cisco IOS Software and ICMP Redirect Issue

Document ID: 59860

Revision 1.0

For Public Release 2002 May 21

Please provide your feedback on this document.

Summary
Details
Cisco Security Procedures

Summary

This document is provided to simplify access to Cisco responses to possible product security vulnerability issues posted in public forums for Cisco customers. This does not imply that Cisco perceives each of these issues as an actual product security vulnerability. This notice is provided on an "as is" basis and does not imply any kind of guarantee or warranty. Your use of the information on the page or materials linked from this page are at your own risk. Cisco reserves the right to change or update this page without notice at any time.

Details

Original Report: <http://www.phenoelit.de/stuff/CiscoICMP.txt>. Cisco responded with the following, which is also archived at <http://www.securityfocus.com/archive/1/273488>.

```
To: BugTraq
Subject: Cisco IOS ICMP redirect DoS - Cisco's response
Date: May 21 2002 5:45PM
Author: Damir Rajnovic <gaus cisco com>
Message-ID: <4.3.2.7.2.20020521184408.02ab79c8@144.254.74.238>
```

-----BEGIN PGP SIGNED MESSAGE-----

Hello,

We can confirm the finding made by FX phenoelit de This issue is assigned Cisco bug ID CSCdx32056. The fix has been developed and it is being committed into all affected releases.

The situation in Cisco IOS 12.x code is that the redirect cache will only grow if "ip routing" is disabled. The Cisco IOS 11.x code will populate the redirect cache ignoring the state of the "ip routing". The redirect cache is fixed in size and an entry timeout is four hours.

By filling the redirect cache the memory is consumed. If the device is already low on memory that may cause further irregularities in the device's performance. Effects can vary, some of them can be: new routes can not be learned, new MAC entries might not be added, Telnet session might not be established, new CDP entries might not be

added. Depending on the exact configuration and circumstances, the device may become totally unresponsive. The device should recover by itself after the four hours when the entries will start to timeout.

The workaround for users running Cisco IOS 11.x code is to block all ICMP redirect messages that are sent to the router itself. That can be accomplished this way:

```
router(config)#access-list 101 deny icmp any host <device_IP> redirect
... (the rest of the access-list 101)
router(config)#interface eth0
router(config-if)#ip access-group 101 in
```

This example will block all ICMP packets, sent to the router itself, coming from the eth0 interface. All transit ICMP redirect packets will be allowed through.

Although, Cisco IOS 12.x code is less exposed we recommend to block all ICMP redirect packets sent to the device itself.

Gaus

```
-----BEGIN PGP SIGNATURE-----
Version: PGP 6.5.3
```

```
iQEVAwUBPOqHtw/VLJ+budTTAQFsvwf/bsR/O6QMhPjxr8sGtQJ58Xr/EC1WkiQn
H0jIPGsm9wv5F4hWlpjRizfVX9GfEoLs8yrknBWXQ08cwB+TizzsSdUVnQXkp4z
6gYzHymdSbvZW/pSJyPa4J0r80MoVN8qOgavD6iCbvlT8GA67lS13YdLHDYos2cP
3c8B8UwXGiOdCJQAI1UY2gg592owahSjXRaTwStitGiwMruhKDQE0sqWDNlh0YPw
B85QJYpds2HrsC31tYO3P0rocToZFvUPA4zd5MaaqZ4gbd1TZDU5p0ktDbnRJZy/
KAFm/YV9yQIFjJzUzmcY7izj+09pr/qNocvAvTw24CGcxGPXX+wDow==
=y3UB
```

```
-----END PGP SIGNATURE-----
```

```
=====
Damir Rajnovic <psirt cisco com>, PSIRT Incident Manager, Cisco Systems
<http://www.cisco.com/go/psirt> Telephone: +44 7715 546 033
200 Longwater Avenue, Green Park, Reading, Berkshire RG2 6GB, GB
=====
```

There is no insolvable problems.
The question is can you accept the solution?

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>.

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: May 21, 2002

Document ID: 59860
