

Cisco Security Response: Cisco IOS GRE Decapsulation Vulnerability

Document ID: 71314

<http://www.cisco.com/warp/public/707/cisco-sr-20060906-gre.sh>

Revision 1.0

For Public Release 2006 September 06 2300 UTC (GMT)

Please provide your feedback on this document.

[Cisco Response](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)

Cisco Response

This is a Cisco response to an advisory published by FX of Phenoelit posted as of September 06, 2006, at <http://www.securityfocus.com/archive/1/445322/30/0/threaded>, and entitled "Cisco Systems IOS GRE decapsulation fault".

This issue is being tracked by the following Cisco bug IDs:

- CSCuk27655 (registered customers only) GRE: make implementation RFC 2784 and RFC 2890 compliant
- CSCea22552 (registered customers only) GRE: implementation of Reserved0 field not RFC2784 compliant
- CSCei62762 (registered customers only) GRE: IP GRE Tunnel with Routing Present Bit not dropped

We would like to thank FX from Phenoelit for reporting this issue to Cisco. We greatly appreciate the opportunity to work with researchers on security vulnerabilities, and welcome the opportunity to review and assist in product reports.

Additional Information

Generic Routing Encapsulation (GRE) is a generic packet encapsulation protocol. GRE is documented in RFC1701 and RFC2784.

Vulnerable Products

- Cisco IOS software 12.0, 12.1, and 12.2 based trains
- All devices running affected versions of Cisco IOS[®] software and configured with GRE IP or GRE IP multipoint tunnels

Products Not Affected by This Vulnerability

- Cisco IOS Software 12.3 and 12.4 based trains
- Cisco IOS Software 12.0S release train, with a revision later than Cisco IOS Software Release 12.0(23)S, with CEF enabled (default behavior)

In RFC1701, the GRE Header field (described in RFC2784 as Reserved0) contains a number of flag bits which RFC2784 deprecates. In particular, the Routing Present and Strict Source Route bits along with Routing Information fields have been deprecated. All versions of Cisco IOS software that support RFC2784 will not be affected by this vulnerability, as any packet where any of the bits 1–5 are non-zero will be discarded.

Cisco IOS software releases that contain ANY of the following three fixes are RFC2784 compliant and are not affected by this vulnerability:

- CSCuk27655 (registered customers only) GRE: make implementation RFC 2784 and RFC 2890 compliant
- CSCea22552 (registered customers only) GRE: implementation of Reserved0 field not RFC2784 compliant
- CSCei62762 (registered customers only) GRE: IP GRE Tunnel with Routing Present Bit not dropped

Vulnerability Impact Overview

Upon receiving a specially crafted GRE packet, depending on the data within a specific packet memory location, the GRE code will decapsulate a packet using the contents of referenced memory buffers.

With **debug tunnel** enabled, output similar as shown below will be produced:

```
GRE decapsulated IP 0.3.74.0->0.0.1.30 (len=65407, ttl=39)
GRE decapsulated IP 176.94.8.0->0.0.0.0 (len=64904, ttl=0)
GRE decapsulated IP 0.15.31.193->176.94.8.0 (len=64894, ttl=237)
GRE decapsulated IP 128.42.131.220->128.0.3.74 (len=64884, ttl=128)
```

Only if the referenced memory buffers data decapsulates to a valid IPv4 packet will this packet be forwarded. Invalid IPv4 packets will be dropped at the router.

This potentially could be used to bypass access-control lists on the router.

Workarounds and Mitigations

The following workaround is applicable to Cisco IOS software 12.0S based trains only:

- Cisco Express Forwarding (CEF)

Running the Cisco IOS software 12.0S release train, with a revision later than Cisco IOS Software Release 12.0(23)S, with CEF enabled, will mitigate this vulnerability. CEF is enabled by default for Cisco IOS software versions 12.0S releases. To check the status of CEF on the router, issue the CLI command **sh ip cef** or **sh ip cef interface**. Refer to http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a0080 for further information on CEF.

The following mitigations may be applied to vulnerable Cisco IOS software releases:

- Anti-spoofing mechanisms of the tunnel source and destination end points:

For further information on deploying anti-spoofing mechanisms, refer to http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml#sec_ip and <http://www.ietf.org/rfc/rfc2827.txt> .

- Encrypt the GRE tunnel with IPSec:

For further information, refer to http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a0080

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	2006–September–06	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>.

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

Updated: Jun 14, 2007

Document ID: 71314
