

# [NEWS] Cisco IOS Misformed BGP Packet Causes Reload

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0126.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 01/27/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 27 Jan 2005 15:10:19 +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>

-----

Cisco IOS Misformed BGP Packet Causes Reload

---

## SUMMARY

A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DoS) attack from a malformed BGP packet. Only devices with the command `bgp log-neighbor-changes` configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet.

Cisco has made free software available to address this problem.

## DETAILS

### Affected Products

### Vulnerable Products

This vulnerability is present in any unfixed version of Cisco IOS, from the beginning of support for the BGP protocol, including versions 9.x, 10.x, 11.x and 12.x. This issue affects all Cisco devices configured for BGP routing and running the `bgp log-neighbor-changes` command, which is on

## Securiteam: [NEWS] Cisco IOS Misformed BGP Packet Causes Reload

by default starting with releases 12.0(22)S, 12.0(11)ST, 12.1(10)E, 12.1(10) and later software.

A router which is running the BGP process will have both a line in the configuration defining the AS number and the command `bgp log-neighbor-changes`, which can be seen by issuing the command `show running-config`:

```
router bgp <AS number>
bgp log-neighbor-changes
```

To determine the software running on a Cisco product, log in to the device and issue the `show version` command to display the system banner. Cisco IOS software will identify itself as "Internetwork Operating System Software" or simply "IOS ." On the next line of output, the image name will be displayed between parentheses, followed by "Version" and the IOS release name. Other Cisco devices will not have the `show version` command or will give different output.

The following example identifies a Cisco product running IOS release 12.0(3) with an installed image name of C2500-IS-L:

```
Cisco Internetwork Operating System Software IOS (TM)
2500 Software (C2500-IS-L), Version 12.0(3), RELEASE SOFTWARE
```

The release train label is "12.0."

The next example shows a product running IOS release 12.0(2a)T1 with an image name of C2600-JS-MZ:

```
Cisco Internetwork Operating System Software IOS (tm)
C2600 Software (C2600-JS-MZ), Version 12.0(2a)T1, RELEASE SOFTWARE (fc1)
```

Additional information about Cisco IOS release naming can be found at:  
<[http:// www.cisco.com/warp/public/620/1.html](http://www.cisco.com/warp/public/620/1.html)> <http://www.cisco.com/warp/public/620/1.html>.

### Products Confirmed Not Vulnerable

Products confirmed not to be vulnerable include devices that do not run Cisco IOS, such as the Cisco Guard, products that cannot participate in BGP or products that cannot be configured for BGP. No other Cisco products are currently known to be affected by this vulnerability.

### Details

The Border Gateway Protocol (BGP) is a routing protocol defined by RFC 1771, and designed to manage IP routing in large networks. An affected Cisco device running a vulnerable version of Cisco IOS software with the BGP protocol enabled will reload if a malformed BGP packet is already queued on the interface when a BGP neighbor change is logged. The device is not vulnerable unless the command `bgp log-neighbor-changes` is

## Securiteam: [NEWS] Cisco IOS Misformed BGP Packet Causes Reload

configured. Malformed packets may not come from malicious sources; a valid peering device such as another BGP speaking router which produces the specific malformed packet in error may trigger this behavior.

BGP runs over the Transport Control Protocol (TCP), a reliable transport protocol which requires a valid three way handshake before any further messages will be accepted. The Cisco IOS implementation of BGP requires the explicit definition of a neighbor before a connection can be established, and traffic must appear to come from that neighbor. These implementation details make it very difficult to maliciously send a BGP packet to a Cisco IOS device from an unauthorized source.

This bug may also be triggered by other means which are not considered remotely exploitable. The use of the commands `show ip bgp neighbors` or `debug ip bgp updates` can cause a router to reload if a router has previously queued a malformed packet. If there are no queued malformed packets, issuing these commands will have no harmful side effects.

A Cisco device receiving an invalid BGP packet will reset and may take several minutes to become fully functional. This vulnerability may be exploited repeatedly resulting in an extended DoS attack. This issue is documented in bug ID CSCee67450 ( registered customers only) .

### Impact

Successful exploitation of this vulnerability results in a reload of the device. Repeated exploitation could result in a sustained DoS attack.

### Software Versions and Fixes

A table listing all the vulnerable versions and their corresponding fixes can be found at:

<<http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml#software>>  
<http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml#software>

### Workarounds

The effectiveness of any workaround is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround is the most appropriate for use in the intended network before it is deployed.

\* Remove the configuration command `bgp log-neighbor-changes`. This feature is used to monitor BGP peer status and its removal may reduce network monitoring capabilities. More information on this command is available here:

<[http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/iprrp\\_r/ip2\\_a1g.htm#wp1040601](http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgr/iprrp_r/ip2_a1g.htm#wp1040601)>  
Cisco IOS IP Routing Protocol Commands

The use of networking best practices techniques can greatly reduce the probability of a network infrastructure attack. Best practices that may reduce risk in this case include:

## Securiteam: [NEWS] Cisco IOS Misformed BGP Packet Causes Reload

### BGP MD5

Under normal circumstances, due to inherent security factors in the TCP protocol, such as sequence number checks, it is difficult, but possible to forge an appropriate packet to exploit this problem. Configuring your Cisco IOS device for BGP MD5 authentication greatly increases the work necessary to forge a valid packet from a remote peer. This will not protect your peering session if a valid BGP peer generates an invalid packet.

This can be configured as shown in the following example:

```
router(config)# router bgp
router(config-router)# neighbor <IP_address> password
<enter_your_secret_here>
```

It is necessary to configure the same shared MD5 secret on both peers and at the same time. Failure to do so will break the existing BGP session and the new session will not get established until the exact same secret is configured on both devices. For a detailed discussion on how to configure BGP, refer to the following document:

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products\\_configuration\\_guide\\_chapter09186a00800ca571](http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_configuration_guide_chapter09186a00800ca571)  
Configuring BGP

Once the secret is configured, it is prudent to change it periodically. The exact period must fit within your company security policy but it should not be longer than a few months. When changing the secret, again it must be done at the same time on both devices. Failure to do so will break your existing BGP session. The exception is if your Cisco IOS software release contains the integrated CSCdx23494 ( registered customers only) fix on both sides of the connection. With this fix, the BGP session will not be terminated when the MD5 secret is changed only on one side. The BGP updates, however, will not be processed until either the same secret is configured on both devices or the secret is removed from both devices.

### Infrastructure Access Control Lists (iACLs)

Although it is often difficult to block traffic transiting your network, it is possible to identify traffic that should never be allowed to target your infrastructure devices and block that traffic at the border of your network. Infrastructure ACLs are considered a network security best practice and should be considered as a long-term addition to good network security as well as providing some added protection for this specific vulnerability. The white paper entitled "Protecting Your Core: Infrastructure Protection Access Control Lists" presents guidelines and recommended deployment techniques for infrastructure protection ACLs:  
<<http://www.cisco.com/warp/public/707/iacl.html>>  
<http://www.cisco.com/warp/public/707/iacl.html>

### ADDITIONAL INFORMATION

Securiteam: [NEWS] Cisco IOS Misformed BGP Packet Causes Reload

The information has been provided by <mailto:psirt@cisco.com> Cisco Systems Product Security Incident Response Team.

The original article can be found at:

<<http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml>>

<http://www.cisco.com/warp/public/707/cisco-sa-20050126-bgp.shtml>

=====

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@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

**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.