

[VulnWatch] Cisco Security Advisory: IOS Stack Group Bidding Protocol Crafted Packet DoS

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-01/msg00032.html>

- *From:* Cisco Systems Product Security Incident Response Team <psirt@xxxxxxxx>
 - *Date:* Wednesday, 18 Jan 2006 10:00:00 -0600
-

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

Hash: SHA1

Cisco Security Advisory: IOS Stack Group Bidding Protocol Crafted Packet DoS

Document ID: 68793

Advisory ID: cisco-sa-20060118-sgbp

<http://www.cisco.com/warp/public/707/cisco-sa-20060118-sgbp.shtml>

Revision 1.0

=====

For Public Release 2006 January 18 1600 UTC (GMT)

Contents

=====

Summary
Affected Products
Details
Impact
Software Versions and Fixes
Workarounds
Obtaining Fixed Software
Exploitation and Public Announcements
Status of This Notice: FINAL
Distribution
Revision History
Cisco Security Procedures

Summary

=====

The Cisco IOS Stack Group Bidding Protocol (SGBP) feature in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable denial of service condition. Devices that do not support or have not enabled the SGBP protocol are not affected by this vulnerability.

Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at
<http://www.cisco.com/warp/public/707/cisco-sa-20060118-sgbp.shtml>

Affected Products

=====

Vulnerable Products

+-----

This vulnerability affects any device that runs Cisco IOS and has enabled the SGBP protocol. SGBP is enabled by defining a stack group, which is done using the global IOS command "sgbp group <name>". The presence of this command will cause the device to begin listening on port 9900, even if the remaining SGBP parameters are not fully configured.

The following examples demonstrate device configurations for which SGBP is enabled:

```
Router#show sgbp
Group Name: test Ref: 0xA3728C00
Seed bid: default, 50, default seed bid setting
```

Or:

```
Router#show running-config | include sgbp
sgbp group test_group
```

If your device displays output similar to either of the above examples, please consult the IOS software table below to determine whether your version of IOS is affected.

Products Confirmed Not Vulnerable

+-----

Cisco products that do not run IOS, do not contain support for SGBP, or do not have SGBP enabled are not affected by this vulnerability.

Systems on which SGBP is not supported or enabled will return either

blank output or an error message. The following examples demonstrate device configurations that are not affected by this vulnerability:

* A system that supports but is not enabled for SGBP returns this output:

```
Router#show sgbp
Router#
```

* A system that does not support SGBP returns this error message:

```
Router#show sgbp
Router#show sgbp
^
% Invalid input detected at '^' marker.
```

Details

=====

Multilink PPP (MLP) allows users to combine multiple PPP links into a single logical network connection, thus enabling on demand bandwidth allocation. When implemented across multiple device chassis, this is known as Multichassis Multilink PPP (MMP). The Stack Group Bidding Protocol is the mechanism by which devices participating in MMP locate each other and negotiate for a connection termination point.

The SGBP implementation provided by the Cisco Internetwork Operating System (IOS) is susceptible to a denial of service attack when presented with a crafted UDP packet. Sending such a packet to port 9900 of an affected device will cause it to freeze and stop responding to or passing traffic. After a delay, the system watchdog timer will detect this condition and force a reset of the device. The system recovery behavior will be controlled by the device configuration register; for example, the router may reload or drop to the ROM monitor.

This vulnerability is documented in Cisco bug ID CSCsb11124.

Impact

=====

Successful exploitation of this vulnerability may cause the affected device to become unresponsive and trigger a hardware reset, resulting in a denial of service condition.

Software Versions and Fixes

=====

Cisco has provided updated software to address this vulnerability. For further details, please refer to the software table below.

[VulnWatch] Cisco Security Advisory: IOS Stack Group Bidding Protocol Crafted Packet DoS

When considering software upgrades, also consult

<http://www.cisco.com/go/psirt>

and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

Each row of the Cisco IOS software table (below) describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix (the "First Fixed Release") and the anticipated date of availability for each are listed in the "Rebuild" and "Maintenance" columns. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

For more information on the terms "Rebuild" and "Maintenance," consult the following URL:

<http://www.cisco.com/warp/public/620/1.html>

Major Release	Availability of Repaired Release	Releases
Affected		
12.0-Based	Rebuild	Maintenance
Release		
12.0	Migrate to 12.2(32)	
12.0(28)S6		
12.0(30)S5		
available		
23-Feb-06		
12.0S	12.0(31)S3	
available		
26-Jan-06		
12.0(32)S		
available		
26-Jan-06		

[VulnWatch] Cisco Security Advisory: IOS Stack Group Bidding Protocol Crafted Packet DoS

| 12.0SC | Migrate to 12.3(13a)BC or |
| | later |
|-----+-----|
| 12.0T | Migrate to 12.2(32) or |
| | later |
|-----+-----|
| 12.0XA | Migrate to 12.2(32) or |
| | later |
|-----+-----|
| 12.0XC | Migrate to 12.2(32) or |
| | later |
|-----+-----|
| 12.0XD | Migrate to 12.2(32) or |
| | later |
|-----+-----|
| 12.0XE | Migrate to 12.1(26)E5 |
|-----+-----|
| 12.0XG | Migrate to 12.2(32) or |
| | later |
|-----+-----|
| 12.0XH | Migrate to 12.2(32) or |
| | later |
|-----+-----|
| 12.0XI | Migrate to 12.2(32) or |
| | later |
|-----+-----|
| 12.0XJ | Migrate to 12.2(32) or |
| | later |
|-----+-----|
| 12.0XK | Migrate to 12.2(32) or |
| | later |
|-----+-----|
| 12.0XL | Migrate to 12.2(32) or |
| | later |
|-----+-----|
| 12.0XN | Migrate to 12.2(32) or |
| | later |
|-----+-----|
| 12.0XR | Migrate to 12.2(32) or |
| | later |
|-----+-----|
Affected		
12.1–Based	Rebuild	Maintenance
Release		
-----+-----		
12.1	Migrate to 12.2(32) or	
	later	
-----+-----		
12.1AA	Migrate to 12.2(32) or	
	later	
-----+-----		

[VulnWatch] Cisco Security Advisory: IOS Stack Group Bidding Protocol Crafted Packet DoS

12.1E		12.1(26)E5		

12.1EC		Migrate to 12.3(13a)BC		or
later				

12.1EX		Migrate to 12.1(26)E5		

12.1EZ		Migrate to 12.1(26)E5		

12.1GA		Migrate to 12.2(32)		or
later				

12.1GB		Migrate to 12.2(32)		or
later				

12.1T		Migrate to 12.2(32)		or
later				

12.1XA		Migrate to 12.2(32)		or
later				

12.1XD		Migrate to 12.2(32)		or
later				

12.1XH		Migrate to 12.2(32)		or
later				

12.1XI		Migrate to 12.2(32)		or
later				

12.1XL		Migrate to 12.3(16)		or
later				

12.1XM		Migrate to 12.3(16)		or
later				

12.1XQ		Migrate to 12.3(16)		or
later				

12.1XS		Migrate to 12.2(32)		or
later				

12.1XU		Migrate to 12.2(32)		or
later				

12.1XW		Migrate to 12.2(32)		or
later				

12.1XX		Migrate to 12.2(32)		or
later				

[VulnWatch] Cisco Security Advisory: IOS Stack Group Bidding Protocol Crafted Packet DoS

```
| 12.1XY | Migrate to 12.2(32) or |
| | later |
|-----+-----|
| 12.1XZ | Migrate to 12.2(32) or |
| | later |
|-----+-----|
| 12.1YA | Migrate to 12.3(16) or |
| | later |
|-----+-----|
| 12.1YB | Migrate to 12.3(16) or |
| | later |
|-----+-----|
| 12.1YD | Migrate to 12.3(16) or |
| | later |
|-----+-----|
| Affected || |
| 12.2-Based | Rebuild | Maintenance |
| Release ||
|-----+-----+-----|
| 12.2 || 12.2(32) |
|-----+-----|
| 12.2B | Migrate to 12.3(11)T9 or |
| | later |
|-----+-----|
| 12.2BC | Migrate to 12.3(13a)BC or |
| | later |
|-----+-----|
| 12.2BW | Migrate to 12.3(16) or |
| | later |
|-----+-----|
| 12.2BY | Migrate to 12.3(11)T9 or |
| | later |
|-----+-----|
| 12.2CX | Migrate to 12.3(13a)BC or |
| | later |
|-----+-----|
| 12.2DD | Migrate to 12.3(11)T9 or |
| | later |
|-----+-----|
| 12.2DX | Migrate to 12.3(11)T9 or |
| | later |
|-----+-----|
| 12.2MC | Migrate to 12.3(11)T9 or |
| | later |
|-----+-----|
| | 12.2(14) ||
| | S16; ||
| | available ||
| | 9-Feb-06 ||
| 12.2S |||
| | 12.2(18)S ||
```

[VulnWatch] Cisco Security Advisory: IOS Stack Group Bidding Protocol Crafted Packet DoS

```
|| and later ||  
|| are not ||  
|| vulnerable. ||  
-----  
| 12.2SU | Migrate to 12.3(14)T6 |  
-----  
| 12.2SY | Migrate to 12.2SXD or |  
| later |  
-----  
| 12.2SZ | Migrate to 12.2S or later |  
-----  
| 12.2T | Migrate to 12.3(16) or |  
| later |  
-----  
| 12.2XA | Migrate to 12.3(16) or |  
| later |  
-----  
| 12.2XB | Migrate to 12.3(16) or |  
| later |  
-----  
| 12.2XC | Migrate to 12.3(11)T9 or |  
| later |  
-----  
| 12.2XF | Migrate to 12.3(13a)BC or |  
| later |  
-----  
| 12.2XG | Migrate to 12.3(16) or |  
| later |  
-----  
| 12.2XK | Migrate to 12.3(16) or |  
| later |  
-----  
| 12.2XL | Migrate to 12.3(16) or |  
| later |  
-----  
| 12.2XS | Migrate to 12.3(16) or |  
| later |  
-----  
| 12.2XT | Migrate to 12.3(16) or |  
| later |  
-----  
| 12.2XV | Migrate to 12.3(16) or |  
| later |  
-----  
| 12.2YD | Migrate to 12.3(11)T9 or |  
| later |  
-----  
| 12.2YE | Migrate to 12.2S or later |  
-----  
| 12.2YN | Migrate to 12.3(11)T9 or |  
| later |
```

[VulnWatch] Cisco Security Advisory: IOS Stack Group Bidding Protocol Crafted Packet DoS

12.2YT	Migrate to 12.3(16) or later
12.2YW	Migrate to 12.3(11)T9 or later
12.2YX	Migrate to 12.3(14)T6
12.2YY	Migrate to 12.3(11)T9 or later
12.2YZ	Migrate to 12.2S or later
12.2ZA	Migrate to 12.2SXD or later
12.2ZB	Migrate to 12.3(11)T9 or later
12.2ZD	Contact TAC
12.2ZE	Migrate to 12.3(16) or later
12.2ZJ	Migrate to 12.3(11)T9 or later
12.2ZN	Migrate to 12.3(11)T9 or later
Affected	
12.3-Based	Rebuild Maintenance Release
12.3	12.3(16)
12.3B	Migrate to 12.3(11)T9 or later
12.3BC	12.3(13a)BC
12.3BW	Migrate to 12.3(11)T9 or later
12.3(11)T9	
12.3T	-----+-----
12.3(14)T6	
12.3XB	Migrate to 12.3(11)T9 or later

[VulnWatch] Cisco Security Advisory: IOS Stack Group Bidding Protocol Crafted Packet DoS

12.3XD	Migrate to 12.3(11)T9 or later
12.3XF	Migrate to 12.3(11)T9 or later
12.3XH	Migrate to 12.3(11)T9 or later
12.3XI	Contact TAC
12.3XJ	Migrate to 12.3(14)YX or later
12.3XM	Migrate to 12.3(14)T6
12.3XQ	Migrate to 12.4(3) or later
12.3XU	Migrate to 12.4(4)T or later
12.3XW	Migrate to 12.3(14)YX or later
12.3YF	Migrate to 12.3(14)YX or later
12.3YG	Contact TAC
12.3YJ	Migrate to 12.3(14)YQ2
12.3YK	Contact TAC
12.3YM	12.3(14)YM4
12.3YQ	12.3(14)YQ2
12.3YT	Contact TAC
12.3YU	Contact TAC
12.3YX	12.3(14)YX
Affected	12.4-Based Rebuild Maintenance Release
12.4(1b)	
12.4	

```
|| 12.4(3) |
|-----+-----+-----|
| 12.4MR || 12.4(4)MR |
|-----+-----+-----|
|| 12.4(2)T3 ||
|12.4T |-----+-----|
|| 12.4(4)T |
|-----+-----+-----|
| 12.4XA || 12.4(2)XA |
|-----+-----+-----|
| 12.4XB || 12.4(2)XB |
+-----+-----+-----+
```

Workarounds

=====

* Configure Access Control Lists (ACLs)

For sites that require the SGBP protocol to be enabled, it may be possible to apply Access Control Lists (ACLs) to prevent untrusted hosts from exploiting this vulnerability. The following extended access-list can be adapted to your network. This example assumes that the SGBP members communicate using the 192.168.10.0 network.

```
access-list 101 permit udp 192.168.10.0 0.0.0.255 192.168.10.0
0.0.0.255 port eq 9900
access-list 101 deny udp any 192.168.10.0 0.0.0.255 port eq
9900
access-list 101 permit ip any any
```

The access-list must then be applied to all interfaces using configuration commands such as:

```
interface ethernet 0/0
ip access-group 101 in
```

* Enable Control Plane Policing

The Control Plane Policy (CoPP) feature may be used to mitigate this vulnerability, as in this example:

```
! Do not police SGBP traffic from the trusted network
access-list 140 deny udp 192.168.10.0 0.0.0.255 any eq 9900
! Police SGBP traffic from untrusted hosts and networks
access-list 140 permit udp any any eq 9900
! Do not police any other type of traffic going to the router
access-list 140 deny ip any any
!
class-map match-all sgbp-class
match access-group 140
```

```
!  
policy-map control-plane-policy  
! Drop all traffic that matches the class "sgbp-class"  
class sgbp-class  
drop  
!  
control-plane  
service-policy input control-plane-policy
```

Note: CoPP is only available on certain platforms and IOS release trains. Additional information on the configuration and use of the CoPP feature can be found at the following URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_white_paper09186a0080211f39.shtml

* Infrastructure ACLs (iACL)

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 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" presents guidelines and recommended deployment techniques for iACLs:

<http://www.cisco.com/warp/public/707/iacl.html>

* Configuring Receive Access Lists (rACLs)

For distributed platforms, rACLs may be an option starting in Cisco IOS Software Versions 12.0(21)S2 for the 12000 series GSR and 12.0(24)S for the 7500 series. The receive access lists protect the device from harmful traffic before the traffic can impact the route processor. Receive path 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 CPU load is distributed to the line card processors and helps mitigate load on the main route processor. The white paper entitled "GSR: Receive Access Control Lists" will help identify and allow legitimate traffic to your device and deny all unwanted packets:

<http://www.cisco.com/warp/public/707/racl.html>

Obtaining Fixed Software

=====

Cisco has made free software available to address this vulnerability for affected customers. Prior to deploying software, customers should consult their maintenance provider or check the software for feature

set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html> or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>

Do not contact either "psirt@xxxxxxxx" or "security-alert@xxxxxxxx" for software upgrades.

Customers with Service Contracts

+-----

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

Customers using Third-party Support Organizations

+-----

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix 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 or fix is the most appropriate for use in the intended network before it is deployed.

Customers without Service Contracts

+-----

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- * +1 800 553 2447 (toll free from within North America)
- * +1 408 526 7209 (toll call from anywhere in the world)
- * e-mail: tac@xxxxxxxx

[VulnWatch] Cisco Security Advisory: IOS Stack Group Bidding Protocol Crafted Packet DoS

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

Exploitation and Public Announcements

=====

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

This vulnerability was discovered during internal testing.

Status of This Notice: FINAL

=====

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.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

Distribution

=====

This advisory is posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20060118-sgbp.shtml>

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- * cust-security-announce@xxxxxxxxxx
- * first-teams@xxxxxxxxxx
- * bugtraq@xxxxxxxxxxxxxxxxxxxxx
- * vulnwatch@xxxxxxxxxxxxxxxxxx
- * cisco@xxxxxxxxxxxxxxxxxxxxx
- * cisco-nsp@xxxxxxxxxxxxxxxxxxxx
- * full-disclosure@xxxxxxxxxxxxxxxxxxxx
- * comp.dcom.sys.cisco@xxxxxxxxxxxxxxxxxxxx

[VulnWatch] Cisco Security Advisory: IOS Stack Group Bidding Protocol Crafted Packet DoS

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the above URL for any updates.

Revision History

=====

```
+-----+
| Revision | | Initial |
| 1.0 | 2006-January-18 | 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>

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.4.0 (SunOS)

iD8DBQFDzm47ezGozzK2tZARAmLxAKDYI8fIszCIrKEPbtngxG5A/3zcS6QCfs0FC

vB8TjPqap9cvnRRPrpNWrQ4=

=BpZb

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

-
- Prev by Date: [*\[VulnWatch\] Cisco Security Advisory: Cisco Call Manager Denial of Service*](#)
 - Next by Date: [*\[VulnWatch\] Fortinet Advisory: BitComet URI Buffer Overflow Vulnerability*](#)
 - Previous by thread: [*\[VulnWatch\] Cisco Security Advisory: Cisco Call Manager Denial of Service*](#)
 - Next by thread: [*\[VulnWatch\] Fortinet Advisory: BitComet URI Buffer Overflow Vulnerability*](#)
 - Index(es):
 - ◆ [*Date*](#)
 - ◆ [*Thread*](#)