



ADVISORIES

cisco-sa-20040420-tcp-ios: Cisco Security Advisory: TCP Vulnerabilities in Multiple IOS-Based Cisco Products
 Published: Apr 20, 2004
 Updated: Apr 20, 2004

-----BEGIN PGP SIGNED MESSAGE-----
 Hash: SHA1

Cisco Security Advisory: TCP Vulnerabilities in Multiple IOS-Based Cisco Products

Revision 1.0

For Public Release 2004 April 20 21:00 UTC (GMT)

 Summary
 =====

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

Affected Products

=====

Products which contain a TCP stack are susceptible to this vulnerability. All Cisco products and models are affected. The severity of the exposure depends upon the protocols and applications that utilize TCP.

This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer), and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router).

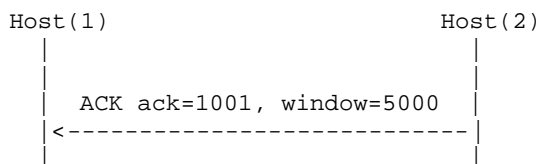
Details

=====

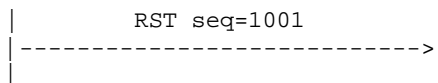
TCP is the transport layer protocol designed to provide connection-oriented reliable delivery of a data stream. To accomplish this, TCP uses a mixture of flags to indicate state and sequence numbers to identify the order in which the packets are to be reassembled. TCP also provides a number, called an acknowledgement number, that is used to indicate the sequence number of the next packet expected. The packets are reassembled by the receiving TCP implementation only if their sequence numbers fall within a range of the acknowledgement number (called a "window"). The acknowledgement number is not used in a packet with the reset (RST) flag set because a reset does not expect a packet in return. The full specification of the TCP protocol can be found at <http://www.ietf.org/rfc/rfc0793.txt>.

According to the RFC793 specification, it is possible to reset an established TCP connection by sending a packet with the RST or synchronize (SYN) flag set. In order for this to occur, the 4-tuple must be known or guessed (source and destination IP address and ports) together with a sequence number. However, the sequence number does not have to be an exact match; it is sufficient to fall within the advertised window. This significantly decreases the effort required by an adversary: the larger the window, the easier it is to reset the connection. While source and destination IP addresses may be relatively easy to determine, the source TCP port must be guessed. The destination TCP port is usually known for all standard services (for example, 23 for Telnet, 80 for HTTP). Cisco IOS software uses predictable ephemeral ports for known services with a predictable increment (the next port which will be used for a subsequent connection). These values, while constant for a particular Cisco IOS software version and protocol, can vary from one release to another.

Here is an example of a normal termination of a TCP session:

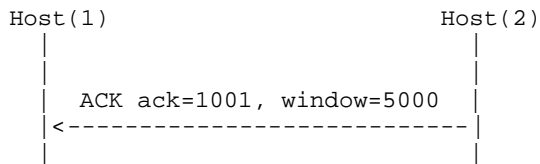


Host(1) is
closing the session

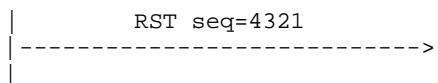


Host(2) is
closing the session

In addition, the following scenario is also permitted:



Host(1) is
closing the session



Host(2) is
closing the session

Note how, in the second example, the RST packet was able to terminate the session although the sequence number was not the next expected one (which is 1001). It was sufficient for the sequence number to fall within the advertised "window". In this example, Host(2) was accepting sequence numbers from 1001 to 6001 and 4321 is clearly within the acceptable range.

As a general rule, all protocols where a TCP connection stays established for longer than one minute should be considered exposed.

The exposure on this vulnerability can be described as follows:

- * Cisco IOS - All devices running Cisco IOS software are vulnerable. Only TCP sessions that are terminating on the device itself are affected since this vulnerability only affects the endpoints of a session. Sessions passing through the device are vulnerable only if the originating or receiving device is vulnerable, but they cannot be attacked on the router itself. This vulnerability does not compromise data integrity or confidentiality. It only affects availability.

This vulnerability is documented in the Cisco Bug Toolkit as Bug IDs CSCed27956 (registered customers only) and CSCed38527 (registered customers only) .

- * Cisco IOS Firewall (IOS FW) - The Cisco IOS FW monitors packets passing through the router and maintains the session state internally. This way, it is possible to "open" required ports and allow traffic to pass and then close them after the session has finished. Since Cisco IOS FW intercepts and examines all packets passing through the device, all TCP sessions passing through the Cisco IOS FW are vulnerable to this attack. This is valid even if the

originating and receiving devices themselves are not vulnerable.

This vulnerability is documented in the Cisco Bug Toolkit as Bug ID CSCed93836 (registered customers only) .

- * Network Address Translation (NAT) - This vulnerability does not have any effect on NAT. The NAT functionality simply rewrites ports and IP addresses. This feature does not interpret TCP flags and therefore is not vulnerable to this attack. However, the attacking packet will be passed through the router and the receiving device can be affected.

Impact

=====

The impact will be different for each specific protocol. While in the majority of cases a TCP connection will be automatically re-established, in some specific protocols a second order of consequences may have a larger impact than tearing down the connection itself.

Border Gateway Protocol (BGP)

- - - - -

The Cisco PSIRT has identified BGP as the protocol which has the greatest potential for impact. Both external and internal (eBGP and iBGP) sessions are equally vulnerable. If an adversary tears down a BGP session between two routers, then all routes which were advertised between these two peers will be withdrawn. This would occur immediately for the router which has been attacked and after the next update/keepalive packet is sent by the other router. The BGP peering session itself will be re-established within a minute after the attack. Depending upon the exact routing configuration, withdrawal of the routes may have any of the following consequences:

- * No adverse effects at all if an appropriate static route(s) has(have) been defined on both sides of the affected session.
- * The traffic will be rerouted along other paths. This may cause some congestion along these paths.
- * A portion of the network will be completely isolated and unreachable.

If a BGP peering session is broken a few times within a short time interval, then BGP route dampening may be invoked. Dampening means that affected routes will be withdrawn from the Internet routing table for some period of time. By default that time is 45 minutes. During that time, all of the traffic whose route was advertised over the attacked BGP session will either be rerouted or a portion of the network will be unreachable. Route dampening is not enabled by default.

Cisco IOS Firewall Feature Set

- - - - -

It is possible to terminate an established TCP-based connection even if both endpoints are not vulnerable to this attack.

Software Versions and Fixes

=====

Each row of the table 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 and the anticipated date of availability for each are listed in the Rebuild, Interim, and Maintenance columns. In some cases, no rebuild of a particular release is planned; this is marked with the label "Not scheduled." A device running any release in the given train that is earlier than the release in a specific column (less than the earliest

fixed release) is known to be vulnerable, and it should be upgraded at least to the indicated release or a later version (greater than the earliest fixed release label).

When selecting a release, keep in mind the following definitions:

* Maintenance

Most heavily tested and highly recommended release of any label in a given row of the table.

* Rebuild

Constructed from the previous maintenance or major release in the same train, it contains the fix for a specific vulnerability. Although it receives less testing, it contains only the minimal changes necessary to effect the repair. Cisco has made available several rebuilds of mainline trains to address this vulnerability, but strongly recommends running only the latest maintenance release on mainline trains.

* Interim

Built at regular intervals between maintenance releases and receives less testing. Interims should be selected only if there is no other suitable release that addresses the vulnerability, and interim images should be upgraded to the next available maintenance release as soon as possible. Interim releases are not available through manufacturing, and usually they are not available for customer download from CCO without prior arrangement with the Cisco Technical Assistance Center (TAC).

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 TAC for assistance, as shown in the section following this table.

Fixed Cisco IOS Software Images for Cisco IOS Firewall

Major Release	Availability of Repaired Releases*		
	Rebuild	Interim	Maintenance
Affected 12.1-Based Release		**	
12.1	12.1 (22c)		
12.1E	12.1 (19)E7		
Affected 12.2-Based Release		**	
12.2	12.2 (21b)		
	12.2 (23a)		

12.2T	12.2 (11)T11		
	12.2 (13)T12		
	12.2 (15)T12		
Affected 12.3-Based Release	Rebuild	Interim **	Maintenance
12.3	12.3 (5c)		
	12.3 (6a)		
12.3T	12.3(4) T4		

Fixed Cisco IOS Software Releases and Migration Path

Major Release	Availability of Repaired Releases*		
Affected -Based Release	Rebuild	Interim **	Maintenance
11.1	11.1 Vulnerable. Migrate to 11.2		
11.1AA	11.1AA Vulnerable. Migrate to 11.2P		
11.1CC	11.1CC Vulnerable. Migrate to 12.0		
Affected -Based Release	Rebuild	Interim **	Maintenance
11.2	11.2(26f) Available on 2004-Apr-21		
11.2P	11.2(26)P6 Available on 2004-Apr-21		
11.2SA	11.2(8)SA6 Vulnerable. Migrate to 12.0		
Affected -Based Release	Rebuild	Interim **	Maintenance
11.3	11.3 Vulnerable. Migrate to 12.0		
	11.3(11b)T4 Available		

	on 2004-Apr-21		
	11.3(11e) Available on 2004-Apr-21		
Affected 12.0 -Based Release	Rebuild	Interim **	Maintenance
12.0	12.0(28)		
12.0DA	12.0DA Vulnerable. Migrate to 12.2DA		
12.0DB	12.0DB Vulnerable. Migrate to 12.1DB		
12.0DC	12.0DC Vulnerable. Migrate to 12.1DC		
12.0S	12.0(27)S		
	12.0(26)S2		
	12.0(16)S11		
	12.0(24)S5		
	12.0(25)S3		
	12.0(23)S6		
12.0SL	12.0SL Vulnerable. Migrate to 12.0 (23)S3		
12.0ST	12.0ST Vulnerable. Migrate to 12.0 (26)S2		
12.0SX	12.0(25)SX4 Not built - contact TAC		
12.0SZ	12.0SZ Vulnerable. Migrate to 12.0 (26)S2		
12.0T	12.0T Vulnerable. Migrate to 12.1		
12.0W5	12.0(28)W5 (30)		
12.0WC	12.0(5)WC9a Available on 2004-Apr-21		
12.0WT	12.0(13)WT Vulnerable. End of Engineering		
12.0WX	12.0(4)WX Vulnerable. Migrate to 12.0W5		
12.0XA	12.0(1)XA Vulnerable. Migrate to 12.1 Latest		
12.0XB	12.0(1)XB Vulnerable. Migrate to		

	12.2(15)T12		
12.0XC	12.0(2)XC Vulnerable. Migrate to 12.1 Latest		
12.0XD	12.0(2)XD Vulnerable. Migrate to 12.1 Latest		
12.0XE	12.0(7)XE Vulnerable. Migrate to 12.1E Latest		
12.0XG	12.0(3)XG Vulnerable. Migrate to 12.1 Latest		
12.0XH	12.0(4)XH Vulnerable. Migrate to 12.1		
12.0XI	12.0(4)XI Vulnerable. Migrate to 12.1		
12.0XJ	12.0(4)XJ Vulnerable. Migrate to 12.1 Latest		
12.0XK	12.0(7)XK Vulnerable. Migrate to 12.1T Latest		
12.0XL	12.0(4)XL Vulnerable. Migrate to 12.2 Latest		
12.0XM	12.0(4)XM Vulnerable. Migrate to 12.2(15)T12		
12.0XN	12.0(5)XN Vulnerable. Migrate to 12.1 Latest		
12.0XP	12.0(5.1)XP Vulnerable. Migrate to 12.1 Latest		
12.0XQ	12.0(5)XQ Vulnerable. Migrate to 12.1 Latest		
12.0XR	12.0(7)XR Vulnerable. Migrate to 12.2 Latest		
12.0XS	12.0(5)XS Vulnerable. Migrate to 12.1E Latest		
12.0XU	12.0(5)XU Vulnerable. Migrate to 12.0(5)WC		
12.0XV	12.0(7)XV Vulnerable. Migrate to 12.2(15)T12		
Affected 12.1 -Based Release	Rebuild	Interim **	Maintenance
12.1	12.1(20a)		
	12.1(4c)		
	12.1(22a)		
12.1AA	12.1(10)AA Vulnerable. Migrate to 12.2 Latest		

12.1AX	12.1(14)AX		
12.1AY	12.1(13)AY Vulnerable. Migrate to 12.1(14)EA1		
12.1DA	12.2DA Vulnerable. Migrate to 12.2DA		
12.1DB	12.1(5)DB Vulnerable. Migrate to 12.2B		
12.1E	12.1(19)E7		
	12.1(22)E1		
	12.1(11b)E14		
	12.1(20)E2	Not built - contact TAC	
	12.1(19)E6		
	12.1(13)E13		
	12.1(8b)E18		
	12.1(14)E10		
	12.1(13)E14		
12.1EA	12.1(20)EA1		
12.1EB	12.1(20)EB		
12.1EC	12.1(20)EC		
12.1EO	12.1(20)EO		
	12.1(19)EO2	Available on 2004-Apr-25	
12.1EU	12.1(20)EU		
12.1EV	12.1(12c)EV Vulnerable. Migrate to 12.2(RLS4)S		
12.1EW	12.1(20)EW2	Available on 2004-Apr-21	
12.1EX	12.1EX Vulnerable. Migrate to 12.1(14)E		
12.1EY	12.1(10)EY Vulnerable. Migrate to 12.1(14)E		
12.1T	12.1(5)T17		
12.1XA	12.1(1)XA Vulnerable. Migrate to 12.1(5)T18		
12.1XB	12.1(1)XB Vulnerable. Migrate to 12.2(15)T12		

12.1XC	12.1(1)XC Vulnerable. Migrate to 12.2
12.1XD	12.1(1)XD Vulnerable. Migrate to 12.2
12.1XE	12.1(1)XE Vulnerable. Migrate to 12.1E Latest
12.1XF	12.1(2)XF Vulnerable. Migrate to 12.2(15)T12
12.1XG	12.1(3)XG Vulnerable. Migrate to 12.2(15)T12
12.1XH	12.1(2a)XH Vulnerable. Migrate to 12.2
12.1XI	12.1(3a)XI Vulnerable. Migrate to 12.2 Latest
12.1XJ	12.1(3)XJ Vulnerable. Migrate to 12.2(15)T12
12.1XL	12.1(3)XL Vulnerable. Migrate to 12.2T Latest
12.1XM	12.1(5)XM Vulnerable. Migrate to 12.2T Latest
12.1XP	12.1(3)XP Vulnerable. Migrate to 12.2(15)T12
12.1XQ	12.1(3)XQ Vulnerable. Migrate to 12.2T Latest
12.1XR	12.1(5)XR Vulnerable. Migrate to 12.2T Latest
12.1XT	12.1(3)XT Vulnerable. Migrate to 12.2(15)T12
12.1XU	12.1(5)XU Vulnerable. Migrate to 12.2T Latest
12.1XV	12.1(5)XV Vulnerable. Migrate to 12.2XB
12.1YA	12.1(5)YA Vulnerable. Migrate to 12.2(8)T
12.1YB	12.1(5)YB Vulnerable. Migrate to 12.2(15)T12
12.1YC	12.1(5)YC Vulnerable. Migrate to 12.2(15)T12
12.1YD	12.1(5)YD Vulnerable. Migrate to 12.2(8)T
12.1YE	12.1(5)YE5 Vulnerable. Migrate to 12.2(2)YC
12.1YF	12.1(5)YF2 Vulnerable. Migrate to 12.2(2)YC
12.1YH	12.1(5)YH2 Vulnerable. Migrate to

	12.2(13)T		
12.1YI	12.1(5)YI2 Vulnerable. Migrate to 12.2(2)YC		
12.1YJ	12.1(11)YJ Vulnerable. Migrate to 12.1EA Latest		
Affected 12.2 -Based Release	Rebuild	Interim **	Maintenance
12.2	12.2(19b)		
	12.2(16f)		
	12.2(21a)		
	12.2(23)		
	12.2(12i)		
	12.2(10g)		
	12.2(13e)		
	12.2(17d)		
	12.2(21b)		
	12.2(23a)		
12.2B	12.2(2)B - 12.2(4)B7 Vulnerable. Migrate to 12.2(13)T12		
	12.2(4)B8 AND FWD Vulnerable. Migrate to 12.3(5a)B1		
12.2BC	12.2(15)BC1C		
12.2BW	12.2(4)BW Vulnerable. Migrate to 12.2(15)T12		
12.2BX	12.2(16)BX2		
12.2BY	12.2(4)BY Vulnerable. Migrate to 12.2(15)B		
	12.2(8)BY Vulnerable. Migrate to 12.2(8)ZB		
	12.2(2)BY Vulnerable. Migrate to 12.2(8)BZ		
12.2BZ	12.2(15)BZ Vulnerable. Migrate to 12.2(16)BX		
12.2CX	12.2(11)CX Vulnerable. Migrate to 12.2(15)BC		
12.2CY	12.2(11)CY Vulnerable. Migrate to 12.2(13)BC1C		
12.2DD	12.2DD Vulnerable. Migrate to 12.2(4)B1		

12.2DX	12.2(1)DX Vulnerable. Migrate to 12.2DD		
	12.2(2)DX Vulnerable. Migrate to 12.2B Latest		
12.2EW	12.2(18)EW		
12.2JA	12.2(13)JA4		
	12.2(13)JA2		
	12.2(11)JA3		
12.2MC	12.2(15)MC1B		
12.2S	12.2(22)S		
	12.2(14)S7		
	12.2(20)S1		
	12.2(20)S3 Available on 2004-Apr-21		
	12.2(18)S3		
12.2SE	12.2(18)SE		
12.2SW	12.2(21)SW		
12.2SX	12.2(17a)SX2		
12.2SXA	12.2(17b)SXA1		
12.2SXB	12.2(17d)SXB1 Not built - contact TAC		
12.2SY	12.2(14)SY3		
12.2SZ	12.2(14)SZ6		
12.2T	12.2(15)T11		
	12.2(13)T12		
	12.2(11)T11 Not built - contact TAC		
	12.2(13)T11		
12.2XA	12.2(2)XA Vulnerable. Migrate to 12.2(11)T		
12.2XB	12.2(2)XB Vulnerable. Migrate to 12.2(15)T		
12.2XC	12.2(2)XC Vulnerable. Migrate to 12.2(8)ZB		
12.2XD	12.2(1)XD Vulnerable. Migrate to 12.2(15)T12		

12.2XE	12.2(1)XE Vulnerable. Migrate to 12.2(15)T12
12.2XF	12.2(1)XF1 Vulnerable. Migrate to 12.2(4)BC1C
12.2XG	12.2(2)XG Vulnerable. Migrate to 12.2(8)T
12.2XH	12.2(2)XH Vulnerable. Migrate to 12.2(15)T12
12.2XI	12.2(2)XI2 Vulnerable. Migrate to 12.2(15)T12
12.2XJ	12.2(2)XJ Vulnerable. Migrate to 12.2(15)T12
12.2XK	12.2(2)XK Vulnerable. Migrate to 12.2(15)T12
12.2XL	12.2(4)XL Vulnerable. Migrate to 12.2(15)T12
12.2XM	12.2(4)XM Vulnerable. Migrate to 12.2(15)T12
12.2XN	12.2(2)XN Vulnerable. Migrate to 12.2(11)T
12.2XQ	12.2(2)XQ Vulnerable. Migrate to 12.2(15)T12
12.2XS	12.2(1)XS Vulnerable. Migrate to 12.2(11)T
12.2XT	12.2(2)XT Vulnerable. Migrate to 12.2(11)T
12.2XU	12.2(2)XU Vulnerable. Migrate to 12.2(15)T12
12.2XW	12.2(4)XW Vulnerable. Migrate to 12.2(13)T12
12.2YA	12.2(4)YA Vulnerable. Migrate to 12.2(15)T12
12.2YB	12.2(4)YB Vulnerable. Migrate to 12.2(15)T12
12.2YC	12.2(2)YC Vulnerable. Migrate to 12.2(11)T11
12.2YD	12.2(8)YD Vulnerable. Migrate to 12.2(8)YY
12.2YE	12.2(9)YE Vulnerable. Migrate to 12.2S
12.2YF	12.2(4)YF Vulnerable. Migrate to 12.2(15)T12
12.2YG	12.2(4)YG Vulnerable. Migrate to 12.2(13)T12

12.2YH	12.2(4)YH Vulnerable. Migrate to 12.2(15)T12
12.2YJ	12.2(8)YJ Vulnerable. Migrate to 12.2(15)T12
12.2YK	12.2(2)YK Vulnerable. Migrate to 12.2(13)ZC
12.2YL	12.2(8)YL Vulnerable. Migrate to 12.3(2)T
12.2YM	12.2(8)YM Vulnerable. Migrate to 12.3(2)T
12.2YN	12.2(8)YN Vulnerable. Migrate to 12.3(2)T
12.2YO	12.2(9)YO Vulnerable. Migrate to 12.2(14)SY
12.2YP	12.2(11)YP Vulnerable. Migrate to 12.2T Latest
12.2YQ	12.2(11)YQ Vulnerable. Migrate to 12.3(2)T
12.2YR	12.2(11)YR Vulnerable. Migrate to 12.3(2)T
12.2YS	12.2(11)YS Vulnerable. Migrate to 12.3T
12.2YT	12.2(11)YT Vulnerable. Migrate to 12.2(15)T
12.2YU	12.2(11)YU Vulnerable. Migrate to 12.3(2)T
12.2YV	12.2(11)YV Vulnerable. Migrate to 12.3(4)T
12.2YW	12.2(8)YW Vulnerable. Migrate to 12.3(2)T
12.2YX	12.2(11)YX Vulnerable. Migrate to 12.2(RLS3)S
12.2YY	12.2(8)YY Vulnerable. Migrate to 12.3(1)T
12.2YZ	12.2(11)YZ Vulnerable. Migrate to 12.2(14)SZ
12.2ZA	12.2(14)ZA6
12.2ZB	12.2(8)ZB Vulnerable. Migrate to 12.3T
12.2ZC	12.2(13)ZC Vulnerable. Migrate to 12.3T
12.2ZD	12.2(13)ZD1
12.2ZE	12.2(13)ZE Vulnerable. Migrate to 12.3

12.2ZF	12.2(13)ZF Vulnerable. Migrate to 12.3(4)T		
12.2ZG	12.2(13)ZG Vulnerable. Migrate to 12.3(4)T		
12.2ZH	12.2(13)ZH Vulnerable. Migrate to 12.3(4)T		
12.2ZI	12.2(11)ZI Vulnerable. Migrate to 12.2(18)S		
12.2ZJ	12.2(15)ZJ5		
	12.2(15)ZJ4		
12.2ZK	12.2(15)ZK Vulnerable. Migrate to 12.3T		
12.2ZL	12.2(15)ZL Vulnerable. Migrate to 12.3(7)T		
12.2ZN	12.2(15)ZN Vulnerable. Migrate to 12.3(2)T		
12.2ZP	12.2(13)ZP3		
Affected 12.3 -Based Release	Rebuild	Interim **	Maintenance
12.3	12.3(3e)		
	12.3(6)		
	12.3(5b)		
12.3B	12.3(5a)B		
	12.3(3)B1		
12.3BW	12.3(1a)BW Vulnerable. Migrate to 12.3B		
12.3T	12.3(2)T4		
	12.3(7)T1 Not built - contact TAC		
	12.3(4)T3		
12.3XA	12.3(2)XA Vulnerable. Contact TAC.		
12.3XB	12.3(2)XB2		
12.3XC	12.3(2)XC2		
12.3XD	12.3(4)XD1		
12.3XE	12.3(2)XE Vulnerable. Migrate to 12.3T		
12.3XF	12.3(2)XF Vulnerable. Contact TAC if needed.		
12.3XG	12.3(4)XG		

12.3XH	12.3(4)XH		
12.3XI	12.3(7)XI	Vulnerable. Migrate to 12.3T	
12.3XJ	12.3(7)XJ	Vulnerable. Contact TAC if needed	
12.3XK	12.3(4)XK		
12.3XL	12.3(7)XL	Vulnerable. Contact Tac if needed	
12.3XM	12.3(9)XM	Vulnerable. Contact TAC if needed.	
12.3XN	12.3(4)XN	Vulnerable. Contact TAC if needed.	
12.3XQ	12.3(4)XQ	Vulnerable. Contact TAC if needed.	
* All dates are estimated and subject to change.			
** Interim releases are subjected to less rigorous testing than regular maintenance releases, and may have serious bugs.			

Obtaining Fixed Software

=====

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 assistance with the upgrade, which should be free of charge.

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@cisco.com

See <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.

Please 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.

Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

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.

There are no workarounds available to mitigate the effects of this vulnerability on Cisco IOS Firewall.

For BGP, we will present the workaround and only a few mitigation techniques. For additional information regarding BGP security risk assessment, mitigation techniques, and deployment best practices, please consult <ftp://ftp-eng.cisco.com/cons/isp/security/BGP-Risk-Assessment-v.pdf>.

* BGP MD5 secret

The workaround for BGP is to configure MD5 secret for each session between peers. This can be configured as shown in the following example:

```
router(config)#router bgp <AS-_number>
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.html. 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. 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.

It is possible to mitigate the exposure for BGP on this vulnerability by applying one or more of the following measures which will lessen the potential for the necessary spoofing required to implement a successful attack:

* 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>, 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 BGP peers. 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
```

Please consult http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7d4.html and <ftp://ftp-eng.cisco.com/cons/isp/security/URPF-ISP.pdf> for further details 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.

- * Packet rate limiting RST packets are rate-limited in Cisco IOS software by default. This feature is introduced in Cisco IOS Software Release 10.2. In the case of a storm of RST packets, they are effectively limited to one packet per second. In order to be successful, an attacker must terminate connection with the first few packets. Otherwise, the attack is deemed to be impracticably long. On the other hand, SYN packets are not rate-limited in any way. Rate limiting can be accomplished either by using Committed Access Rate (CAR) or by Control Plane Policing (CPP). While CPP is the recommended approach, it is available only for Cisco IOS Software Releases 12.2(18)S and 12.3(4)T. It is currently supported only on the following routers: 1751, 2600/2600-XM, 3700, 7200, and 7500 Series.

CAR can be configured as follows:

```
router(config)#access-list 103 deny tcp any host 10.1.1.1 established

router(config)#access-list 103 permit tcp any host 10.0.0.1

router(config)#interface <interface> <interface #>

router(config-if)#rate-limit input access-group 103 8000 8000 8000
conform-action transmit exceed-action drop
```

For details on how to configure and deploy CPP, please consult the following document <http://www.cisco.com/en/US/products/sw/iosswrel/>

ps1838/products_white_paper09186a0080211f39.shtml

Exploitation and Public Announcements

=====

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

The exploitation of the vulnerability with packets having RST flag set (reset packets) was discovered by Paul (Tony) Watson of OSVDB.org. The extension of the attack vector to packets with SYN flag was discovered by the vendors cooperating on the resolution of this issue.

Status of This Notice: INTERIM

=====

This is a INTERIM advisory. Although Cisco cannot guarantee the accuracy of all statements in this advisory, all of the facts have been checked to the best of our ability. Cisco does not anticipate issuing updated versions of this advisory unless there is some material change in the facts. Should there be a significant change in the facts, Cisco may update this advisory.

A stand-alone copy or Paraphrase of the text of this Security Advisory 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 will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.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@cisco.com
- * first-teams@first.org (includes CERT/CC)
- * bugtraq@securityfocus.com
- * vulnwatch@vulnwatch.org
- * cisco@spot.colorado.edu
- * cisco-nsp@puck.nether.net
- * full-disclosure@lists.netsys.com
- * comp.dcom.sys.cisco@newsgate.cisco.com

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	2004-Apr-20	Initial public
1.0		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/warp/public/707/sec_incident_response.shtml. 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 © 1992-2004 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.2.3 (Cygwin)

iD8DBQFAhZTpezGozzK2tZARakKXAJ9BWwuytT7zwoOL+RkZJPebYN3W3ACfV/+K
0Fd3MvvRlKSETCrlMGL/dZg=
=eDSn
-----END PGP SIGNATURE-----

Privacy Statement

Copyright © 1999-2004 SecurityFocus