

Cisco Security Advisory: IPv6 Routing Header Vulnerability

Advisory ID: [cisco-sa-20070124-IOS-IPv6](#)

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml>

1.1

Last Updated 2007 January 27 1645 UTC (GMT)

For Public Release 2007 January 24 1600 UTC (GMT)

Please provide your **feedback** on this document.

Contents

- [Summary](#)
- [Affected Products](#)
- [Details](#)
- [Impact](#)
- [Software Version and Fixes](#)
- [Workarounds](#)
- [Obtaining Fixed Software](#)
- [Exploitation and Public Announcements](#)
- [Status of this Notice:FINAL](#)
- [Distribution](#)
- [Revision History](#)
- [Cisco Security Procedures](#)

Summary

Processing a specially crafted IPv6 Type 0 Routing header can crash a device running Cisco IOS software. This vulnerability does not affect IPv6 Type 2 Routing header which is used in mobile IPv6. IPv6 is not enabled by default in Cisco IOS.

Cisco has made free software available to address this vulnerability for affected customers.

There are workarounds available to mitigate the effects of the vulnerability. The workaround depends on if Mobile IPv6 is used and what version on Cisco IOS is being currently used.

This vulnerability was initially reported by a customer and further trigger vector was discovered during developing the fix for this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml>.

Affected Products

Devices running Cisco IOS and having IPv6 enabled on, at least, one of their interface may be affected by this vulnerability.

Vulnerable Products

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 12.4(9.10):

```
Cisco IOS Software, 7200 Software (C7200-JK9O3S-M), Version 12.4(9.10), INTERIM
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2006 by Cisco Systems, Inc.
Compiled Mon 29-May-06 04:42 by prod_rel_team
```

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

Products Confirmed Not Vulnerable

No other Cisco products are known to be vulnerable to the issue described in this Advisory. In particular Cisco IOS XR, Cisco PIX Appliance and Cisco MDS 9000 Series devices are not affected by this vulnerability.

Details

This vulnerability can be triggered only when Cisco IOS processes specifically crafted IPv6 Type 0 Routing headers, which are used for source routing. Source routing is when an originator node explicitly specifies the exact path that a packet must take to reach the destination. Source routing is enabled by default on Cisco IOS if IPv6 is configured on the device. In order to trigger this vulnerability the packet must be destined to any of the IPv6 addresses defined on the device. The exact packet type is not relevant (e.g., TCP, ICMP, UDP) as the vulnerability is on the IP layer. For this reason care must be taken when implementing a workaround as this vulnerability can be triggered by a spoofed packet.

IPv6 multicast packets can not be used to trigger this vulnerability.

In addition to Type 0 Routing headers, IPv6 also supports Type 2 Routing that is used in Mobile IPv6 implementation. Type 2 Routing headers can not be used to trigger the vulnerability described in this Advisory.

A router running vulnerable Cisco IOS software will process Type 0 Routing headers only if the destination address in the IPv6 packet is one of the IPv6 addresses defined on any of the interfaces. The address may be either a global (i.e., routable), loopback or link local address. Link local addresses are not supposed to be routable and they are valid only among directly connected devices.

A device may also be susceptible in scenarios where IPv6 packets are tunneled over IPv4 networks provided that the IPv6 destination address (after de-encapsulation) is one of the IPv6 addresses defined on the device. This is independent of the exact encapsulation method used (e.g., MPLS, GRE or IPv6-in-IPv4).

This vulnerability is documented in Cisco Bug IDs [CSCsd40334](#) ([registered](#) customers only) and [CSCsd58381](#) ([registered](#) customers only) .

Vulnerability Scoring Details

Cisco is providing scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS).

Cisco will provide a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco PSIRT will set the bias in all cases to normal. Customers are encouraged to apply the bias parameter when determining the environmental impact of a particular vulnerability.

CVSS is a standards based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided an FAQ to answer additional questions regarding CVSS at <http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at <http://intellishield.cisco.com/security/alertmanager/cvss>.

CSCsd40334 - IPv6 packet can cause crash (registered customers only)						
CVSS Base Score - 10						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	Low	Not Required	Complete	Complete	Complete	Normal
CVSS Temporal Score - 8.3						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

CSCsd58381 - IPv6 routing header limitation (registered customers only)						
CVSS Base Score - 10						
Access	Access		Confidentiality	Integrity	Availability	Impact

Vector	Complexity	Authentication	Impact	Impact	Impact	Bias
Remote	Low	Not Required	Complete	Complete	Complete	Normal
CVSS Temporal Score - 8.3						
Exploitability		Remediation Level		Report Confidence		
Functional		Official Fix		Confirmed		

Impact

Successful exploitation of the vulnerability listed in this Advisory can corrupt some memory structures. In most cases this will cause the affected device to crash and repeated exploitation could result in a sustained DoS attack. However, due to memory corruption, there is a potential to execute an arbitrary code. In the event of a successful remote code execution, device integrity will have been completely compromised.

Software Version and Fixes

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>.

Note: There are three IOS security advisories and one field notice being published on January 24, 2007. Each advisory only lists the releases which fix the issue described in the advisory. A combined software table is available at <http://www.cisco.com/warp/public/707/cisco-sa-20070124-bundle.shtml> and can be used to choose a software release which fixes all security vulnerabilities published as of January 24, 2007. The advisories and field notice published on January 24 are listed here.

- <http://www.cisco.com/warp/public/707/cisco-air-20070124-IOS-ipv6.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml>
- <http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml>
- <http://www.cisco.com/warp/customer/770/fn62613.shtml>

Requests for software rebuilds to include the change for [Daylight Savings Time \(DST\)](#) that will be

implemented in March 2007 should be directed through the Technical Assistance Center (TAC) and this advisory should be used as reference.

Major Release	Availability of Repaired Releases	
	Rebuild	Maintenance
Affected 12.0-Based Release		
12.0	Not vulnerable	
12.0DA	Not vulnerable	
12.0DB	Not vulnerable	
12.0DC	Not vulnerable	
12.0S	12.0(32) S3	
12.0SC	Not vulnerable	
12.0SL	Not vulnerable	
12.0SP	Not vulnerable	
12.0ST	Vulnerable; migrate to 12.0(32) S3 or later	
12.0SX	Vulnerable for only 12.0(30)SX; contact TAC	
12.0SY		12.0(32)SY
12.0SZ	Vulnerable; migrate to 12.0(32) S3 or later	
12.0T	Not vulnerable	
12.0W	Not vulnerable	
12.0WC	Not vulnerable	
12.0WT	Not vulnerable	
12.0XA	Not vulnerable	
12.0XB	Not vulnerable	
12.0XC	Not vulnerable	
12.0XD	Not vulnerable	
12.0XE	Not vulnerable	
12.0XF	Not vulnerable	
12.0XG	Not vulnerable	
12.0XH	Not vulnerable	
12.0XI	Not vulnerable	

12.0XJ	Not vulnerable	
12.0XK	Not vulnerable	
12.0XL	Not vulnerable	
12.0XM	Not vulnerable	
12.0XN	Not vulnerable	
12.0XQ	Not vulnerable	
12.0XR	Not vulnerable	
12.0XS	Not vulnerable	
12.0XV	Not vulnerable	
12.0XW	Not vulnerable	
Affected 12.1-Based Release	Rebuild	Maintenance
12.1	Not vulnerable	
12.1AA	Not vulnerable	
12.1AX	Not vulnerable	
12.1AY	Not vulnerable	
12.1AZ	Not vulnerable	
12.1CX	Not vulnerable	
12.1DA	Not vulnerable	
12.1DB	Not vulnerable	
12.1DC	Not vulnerable	
12.1E	Not vulnerable	
12.1EA	Not vulnerable	
12.1EB	Not vulnerable	
12.1EC	Not vulnerable	
12.1EO	Not vulnerable	
12.1EU	Not vulnerable	
12.1EV	Not vulnerable	
12.1EW	Not vulnerable	
12.1EX	Not vulnerable	
12.1EY	Not vulnerable	
12.1EZ	Not vulnerable	
12.1T	Not vulnerable	
12.1XA	Not vulnerable	

12.1XB	Not vulnerable
12.1XC	Not vulnerable
12.1XD	Not vulnerable
12.1XE	Not vulnerable
12.1XF	Not vulnerable
12.1XG	Not vulnerable
12.1XH	Not vulnerable
12.1XI	Not vulnerable
12.1XJ	Not vulnerable
12.1XL	Not vulnerable
12.1XM	Not vulnerable
12.1XP	Not vulnerable
12.1XQ	Not vulnerable
12.1XR	Not vulnerable
12.1XS	Not vulnerable
12.1XT	Not vulnerable
12.1XU	Vulnerable; migrate to 12.3(18) or later
12.1XV	Vulnerable; migrate to 12.3(18) or later
12.1XW	Not vulnerable
12.1XX	Not vulnerable
12.1XY	Not vulnerable
12.1XZ	Not vulnerable
12.1YA	Not vulnerable
12.1YB	Vulnerable; migrate to 12.3(18) or later
12.1YC	Vulnerable; migrate to 12.3(18) or later
12.1YD	Vulnerable; migrate to 12.3(18) or later
12.1YE	Not vulnerable
12.1YF	Not vulnerable
12.1YH	Not vulnerable
12.1YI	Not vulnerable

12.1YJ	Not vulnerable	
Affected 12.2-Based Release	Rebuild	Maintenance
12.2	Not vulnerable	
12.2B	Vulnerable; migrate to 12.3(4) T13 or later	
12.2BC	Vulnerable; migrate to 12.3(17b) BC3 or later	
12.2BW	Vulnerable; migrate to 12.3(18) or later	
12.2BY	Vulnerable; migrate to 12.3(4) T13 or later	
12.2BZ	Not vulnerable	
12.2CX	Vulnerable; migrate to 12.3(17b) BC3 or later	
12.2CY	Not vulnerable	
12.2CZ	Not vulnerable	
12.2DA	Not vulnerable	
12.2DD	Vulnerable; migrate to 12.3(4) T13 or later	
12.2DX	Vulnerable; migrate to 12.3(4) T13 or later	
12.2EU	Vulnerable; migrate to 12.2(25) EWA6 or later	
12.2EW	Vulnerable; migrate to 12.2(25) EWA6 or later	
12.2EWA	12.2(25) EWA6	
12.2EX	Not vulnerable	
12.2EY	Not vulnerable	
12.2EZ	Vulnerable; migrate to 12.2(25) SEE1 or later	
12.2FX	Not vulnerable	
12.2FY	Not vulnerable	
12.2FZ	Not vulnerable	
12.2IXA	Vulnerable; migrate to 12.2(18) IXB or later	
12.2IXB	All 12.2IXB releases are fixed	

12.2IXC	All 12.2IXC releases are fixed	
12.2JA	Not vulnerable	
12.2JK	Not vulnerable	
12.2MB	Not vulnerable	
12.2MC	12.2(15) MC2h	
12.2S	12.2(25) S11	12.2(30)S
12.2SB	12.2(28) SB2	12.2(31)SB
12.2SBC	12.2(27) SBC4	
12.2SEA	Vulnerable; migrate to 12.2(25) SEE1 or later	
12.2SEB	Vulnerable; migrate to 12.2(25) SEE1 or later	
12.2SEC	Vulnerable; migrate to 12.2(25) SEE1 or later	
12.2SED	Vulnerable; migrate to 12.2(25) SEE1 or later	
12.2SEE	12.2(25) SEE1	
12.2SEF	12.2(25) SEF1	
12.2SEG	All 12.2SEG releases are fixed	
12.2SG	12.2(25) SG1	12.2(31)SG
12.2SGA	All 12.2SGA releases are fixed	
12.2SO	Not vulnerable	
12.2SRA	All 12.2SRA releases are fixed	
12.2SRB	All 12.2SRB releases are fixed	
12.2SU	Vulnerable; migrate to 12.3(14) T7 or later	
12.2SV	12.2(25) SV3	12.2(26)SV
12.2SW	12.2(25) SW7	
12.2SX	Vulnerable; migrate to 12.2(18) SXD7a or later	

12.2SXA	Vulnerable; migrate to 12.2(18) SXD7a or later	
12.2SXB	Vulnerable; migrate to 12.2(18) SXD7a or later	
12.2SXD	12.2(18) SXD7a	
12.2SXE	12.2(18) SXE6	
12.2SXF	12.2(18) SXF5	
12.2SY	Vulnerable; migrate to 12.2(18) SXD7a or later	
12.2SZ	Vulnerable; migrate to 12.2(25) S11 or later	
12.2T	Vulnerable; migrate to 12.3(18) or later	
12.2TPC	Vulnerable; contact TAC	
12.2XA	Vulnerable; migrate to 12.3(18) or later	
12.2XB	Vulnerable; migrate to 12.3(18) or later	
12.2XC	Vulnerable; migrate to 12.3(4) T13 or later	
12.2XD	Vulnerable; migrate to 12.3(18) or later	
12.2XE	Not vulnerable	
12.2XF	Vulnerable; migrate to 12.3(17b) BC3 or later	
12.2XG	Vulnerable; migrate to 12.3(18) or later	
12.2XH	Vulnerable; migrate to 12.3(18) or later	
12.2XI	Vulnerable; migrate to 12.3(18) or later	
12.2XJ	Vulnerable; migrate to 12.3(18) or later	
12.2XK	Vulnerable; migrate to 12.3(18) or later	
12.2XL	Vulnerable; migrate to 12.3(18) or later	

12.2XM	Vulnerable; migrate to 12.3(18) or later	
12.2XN		12.2(31)XN
12.2XQ	Vulnerable; migrate to 12.3(18) or later	
12.2XR	Not vulnerable	
12.2XS	Vulnerable; migrate to 12.3(18) or later	
12.2XT	Vulnerable; migrate to 12.3(18) or later	
12.2XU	Vulnerable; migrate to 12.3(18) or later	
12.2XV	Vulnerable; migrate to 12.3(18) or later	
12.2XW	Vulnerable; migrate to 12.3(18) or later	
12.2YA	Vulnerable; migrate to 12.3(18) or later	
12.2YB	Vulnerable; migrate to 12.3(18) or later	
12.2YC	Not vulnerable	
12.2YD	Vulnerable; migrate to 12.3(11) T10 or later	
12.2YE	Vulnerable; migrate to 12.2(25) S11 or later	
12.2YF	Vulnerable; migrate to 12.3(18) or later	
12.2YG	Not vulnerable	
12.2YH	Vulnerable; migrate to 12.3(18) or later	
12.2YJ	Vulnerable; migrate to 12.3(18) or later	
12.2YK	Not vulnerable	
12.2YL	Vulnerable; migrate to 12.3(4) T13 or later	
12.2YM	Vulnerable; migrate to 12.3(4) T13 or later	
12.2YN	Vulnerable; migrate to 12.3(4) T13 or later	

12.2YO	Not vulnerable
12.2YP	Not vulnerable
12.2YQ	Vulnerable; migrate to 12.3(4) T13 or later
12.2YR	Vulnerable; migrate to 12.3(4) T13 or later
12.2YS	Vulnerable; migrate to 12.3(4) T13 or later
12.2YT	Vulnerable; migrate to 12.3(18) or later
12.2YU	Vulnerable; migrate to 12.3(4) T13 or later
12.2YV	Vulnerable; migrate to 12.3(4) T13 or later
12.2YW	Vulnerable; migrate to 12.3(4) T13 or later
12.2YX	Vulnerable; migrate to 12.3(14) T7 or later
12.2YY	Vulnerable; migrate to 12.3(4) T13 or later
12.2YZ	Vulnerable; migrate to 12.2(25) S11 or later
12.2ZA	Vulnerable; migrate to 12.2(18) SXD7a or later
12.2ZB	Vulnerable; migrate to 12.3(4) T13 or later
12.2ZC	Not vulnerable
12.2ZD	Vulnerable; contact TAC
12.2ZE	Vulnerable; migrate to 12.3(18) or later
12.2ZF	Vulnerable; migrate to 12.3(4) T13 or later
12.2ZG	Not vulnerable
12.2ZH	Vulnerable; contact TAC
12.2ZJ	Vulnerable; migrate to 12.3(4) T13 or later
12.2ZL	Vulnerable; contact TAC
12.2ZN	Vulnerable; migrate to 12.3(4) T13 or later

12.2ZP	Not vulnerable	
Affected 12.3-Based Release	Rebuild	Maintenance
12.3	12.3 (17b)	12.3(18)
12.3B	Vulnerable; migrate to 12.3(11) T10 or later	
12.3BC	12.3 (17b) BC3	
12.3BW	Vulnerable; migrate to 12.3(11) T10 or later	
12.3JA	Not vulnerable	
12.3JEA	All 12.3JEA releases are fixed	
12.3JEB	All 12.3JEA releases are fixed	
12.3JK	Not vulnerable	
12.3JX	Not vulnerable	
12.3T	12.3(4) T13	
	12.3(11) T10	
	12.3(14) T7	
	Limited platform support is available: Contact TAC	
	Please migrate to 12.4 (8) or later	
12.3TPC	Not vulnerable	
12.3XA	Vulnerable; contact TAC	
12.3XB	Vulnerable; migrate to 12.3(11) T10 or later	
12.3XC	Vulnerable; contact TAC	

12.3XD	Vulnerable; migrate to 12.3(11) T10 or later	
12.3XE	Vulnerable; contact TAC	
12.3XF	Vulnerable; migrate to 12.3(11) T10 or later	
12.3XG	Vulnerable; contact TAC	
12.3XH	Vulnerable; migrate to 12.3(11) T10 or later	
12.3XI	12.3(7) XI8a	12.3(7)XI9
12.3XJ	Vulnerable; migrate to 12.3(14) YX2 or later	
12.3XK	Vulnerable; migrate to 12.3(14) T7 or later	
12.3XQ	Vulnerable; migrate to 12.4(8) or later	
12.3XR	Vulnerable; contact TAC	
12.3XS	Vulnerable; migrate to 12.4(8) or later	
12.3XU	Vulnerable; migrate to 12.4(2)T4 or later	
12.3XW	Vulnerable; migrate to 12.3(14) YX2 or later	
12.3XX	Vulnerable; migrate to 12.4(8) or later	
12.3XY	Not vulnerable	
12.3YA	Vulnerable; contact TAC	
12.3YD	Vulnerable; migrate to 12.4(2)T4 or later	
12.3YF	Vulnerable; migrate to 12.3(14) YX2 or later	
12.3YG	Vulnerable; migrate to 12.4(2)T4 or later	
12.3YH	Vulnerable; migrate to 12.4(2)T4 or later	
12.3YI	Vulnerable; migrate to 12.4(2)T4 or later	
12.3YJ	Vulnerable; migrate to 12.4(6)T1 or later	

12.3YK	Vulnerable; migrate to 12.4(4)T2 or later	
12.3YM	12.3(14)YM8	
12.3YQ	Vulnerable; migrate to 12.4(6)T1 or later	
12.3YS	Vulnerable; migrate to 12.4(4)T2 or later	
12.3YT	Vulnerable; migrate to 12.4(4)T2 or later	
12.3YU	Vulnerable; migrate to 12.4(2)XB2 or later	
12.3YX	12.3(14)YX2	
12.3YZ	12.3(11)YZ1	
Affected 12.4-Based Release	Rebuild	Maintenance
12.4	12.4(3d)	
	12.4(5b)	
	12.4(7a)	12.4(8)
12.4MR	Not vulnerable	
12.4SW	All 12.4SW releases are fixed	
12.4T	12.4(2)T4	
	12.4(4)T2	
	12.4(6)T1	12.4(9)T
12.4XA	Vulnerable; migrate to 12.4(6)T1 or later	
12.4XB	12.4(2)XB2	
12.4XC	12.4(4)XC5	
12.4XD	12.4(4)XD2	
12.4XE	All 12.4XE releases are fixed	
12.4XG	All 12.4XG releases are fixed	

12.4XJ	All 12.4XJ releases are fixed
12.4XP	All 12.4XP releases are fixed
12.4XT	All 12.4XT releases are fixed

Workarounds

The workaround consists of filtering packets that contain Type 0 Routing header(s). Special attention must be paid not to filter packets with Type 2 Routing headers as that would break Mobile IPv6 deployment. Depending on what Cisco IOS software release is used and if Mobile IPv6 is deployed or not we have the following workarounds. As any packet type can be used to trigger this vulnerability the care must be taken when implementing a workaround to account for a spoofed packet.

Additional mitigations that can be deployed on Cisco devices within the network are available in the Cisco Applied Intelligence companion document for this advisory:

<http://www.cisco.com/warp/public/707/cisco-air-20070124-IOS-IPv6.shtml>

Mobile IPv6 is not deployed

For IOS releases before 12.3(4)T the workaround is to use ACLs to filter all packets that contain Routing headers. This method can not distinguish between Type 0 and Type 2 Routing headers so it is not suitable if Mobile IPv6 is deployed.

The following example shows how to configure such ACLs.

```
Router(config)#ipv6 access-list deny-sourcerouted
Router(config-ipv6-acl)#deny ipv6 any <myaddress1> routing
Router(config-ipv6-acl)#deny ipv6 any <myaddress2> routing
Router(config-ipv6-acl)#permit ipv6 any any
Router(config-ipv6-acl)#exit
Router(config)#interface Ethernet0
Router(config-if)#ipv6 traffic-filter deny-sourcerouted in
```

In this example **<myaddressX>** is an IPv6 address. One example of such address is **3ffe:ffff::/64**. The ACL must be applied to all interfaces and all IPv6 addresses that are configured. If an interface has more than one IPv6 address configured then all addresses must be covered by the ACLs. This also includes all loopback and "link local" addresses for each interface.

The alternative of enumerating all IPv6 addresses is to use statement **deny ipv6 any any routing**. While that simplifies the resulting ACL it will also filter all transit IPv6 traffic with Routing headers 0 and 2. The example where all configured IPv6 addresses are enumerated will not affect transit traffic. This comment is applicable to all other examples in this Advisory.

Starting from the IOS release 12.2(15)T a new command **ipv6 source-route** was introduced. If applied, it will block any IPv6 packet with any IPv6 routing headers (both types 0 and 2). The configuration is given in the following example.

```
Router(config)#no ipv6 source-route
```

This is a global command and it applies to all interfaces. The command is applicable on all defined IPv6

addresses, including the link local and loopback address, and on all interfaces.

Mobile IPv6 is deployed

There is no workaround if you are running a Cisco IOS release prior to 12.4(2)T. In IOS 12.4(2)T a new keyword **routing-type** is added to IPv6 ACLs. It can be used to selectively permit or deny specific routing types.

```
Router(config)#ipv6 access-list deny-sourcerouted
Router(config-ipv6-acl)#deny ipv6 any <myaddress1> routing-type 0
Router(config-ipv6-acl)#permit ipv6 any any
Router(config)#interface Ethernet0
Router(config-if)#ipv6 source-route
Router(config-if)#ipv6 traffic-filter deny-sourcerouted in
```

The filter must be applied to all interfaces that have IPv6 configured.

Obtaining Fixed Software

Cisco will make free software available to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. 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@cisco.com" or "security-alert@cisco.com" 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@cisco.com

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 initially reported to Cisco by Arnaud Ebalard from EADS Corporate Research Center. An additional vector to trigger it was discovered internally while fixing the vulnerability.

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-20070124-IOS-IPv6.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
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- 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

1.1	2007-January-27	Updated Cisco IOS software table.
1.0	2007-January-24	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>.

Help us help you.

Please rate this document.

- Excellent
 Good
 Average
 Fair
 Poor

This document solved my problem.

- Yes
 No
 Just browsing

Suggestions for improvement:

(256 character limit)



Send

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

All contents are Copyright © 1992-2006 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).