

Cisco Security Advisory: Cisco IOS Software SNMP Read–Write ILMI Community String Vulnerability

Document ID: 13630

Advisory ID: cisco–sa–20010227–ios–snmp–ilmi

<http://www.cisco.com/warp/public/707/cisco–sa–20010227–ios–snmp–ilmi.shtml>

Revision 1.5

Last Update 2001 March 07 2200 UTC (GMT)

For Public Release 2001 February 27 0900 UTC (GMT)

Please provide your feedback on this document.

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

Summary

Cisco IOS® Software releases based on versions 11.x and 12.0 contain a defect that allows a limited number of SNMP objects to be viewed and modified without authorization using a undocumented ILMI community string. Some of the modifiable objects are confined to the MIB–II system group, such as "sysContact", "sysLocation", and "sysName", that do not affect the device's normal operation but that may cause confusion if modified unexpectedly. The remaining objects are contained in the LAN–EMULATION–CLIENT and PNNI MIBs, and modification of those objects may affect ATM configuration. An affected device might be vulnerable to a denial–of–service attack if it is not protected against unauthorized use of the ILMI community string.

The vulnerability is only present in certain combinations of IOS releases on Cisco routers and switches. ILMI is a necessary component for ATM, and the vulnerability is present in every IOS release that contains the supporting software for ATM and ILMI without regard to the actual presence of an ATM interface or the physical ability of the device to support an ATM connection.

To remove this vulnerability, Cisco is offering free software upgrades for all affected platforms. The defect is documented in DDTS record CSCdp11863.

In lieu of a software upgrade, a workaround can be applied to certain IOS releases by disabling the ILMI community or "***ilmi**" view and applying an access list to prevent unauthorized access to SNMP. Any affected system, regardless of software release, may be protected by filtering SNMP traffic at a network perimeter or on individual devices.

This notice will be posted at
<http://www.cisco.com/warp/public/707/cisco-sa-20010227-ios-snmp-ilmi.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

The vulnerability is present only in certain releases of Cisco IOS Software versions 11.x and 12.0 for router and switch products that include support for Asynchronous Transfer Mode (ATM) networking and Interim Local Management Interface (ILMI), and it is present without regard to any physical capability for supporting an ATM interface.

Cisco IOS Software versions based on 10.3 and earlier do not contain the vulnerability. The defect was introduced in 11.0(0.2). All Cisco IOS software releases of 12.1 and later have been repaired and are not vulnerable to the defect described in this advisory.

To determine the software running on a Cisco product, log in to the device and issue the command "**show version**" to display the system banner. Cisco IOS software will identify itself as "Internetwork Operating System Software" or simply "IOS (tm)". The image name will be displayed between parentheses, usually on the next line of output, 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
```

Cisco devices that may be running an affected IOS software release include, but are not limited to:

- Cisco 1400 and 1700 series.
- Cisco 2600 (except that c2600-c-mz, c2600-d-mz, c2600-i-mz, c2600-io3-mz, and c2600-ix-mz images are not vulnerable).
- Catalyst 2900 ATM, 2900XL, and 2948g series.
- Cisco 3620 (except that c3620-d-mz, c3620-i-mz, c3620-io3-mz, and c3620-ix-mz images are not vulnerable).
- Cisco 3640 (except that c3640-d-mz, c3640-i-mz, c3640-io3-mz, and c3640-ix-mz images are not vulnerable).
- Cisco 3660 (except that c3660-d-mz, c3660-i-mz, and c3660-ix-mz images are not vulnerable).
- Cisco MC3810 (except that mc3810-i-mz, mc3810-is-mz, mc3810-is56i-mz, and mc3810-js-mz images are not vulnerable).
- Catalyst 4232, 4840g, 5000 RSFC series switches.

- Cisco 4500, 4700, and 5800 DSC series.
- Cisco 6200, 6400 NRP, and 6400 NSP series.
- Catalyst MSM (c6msm), 6000 Hybrid Mode (c6msfc), and 6000 Native Mode (c6sup).
- Cisco RSM, 7000, 7010, 7100, 7200, ubr7200, and 7500 series.
- Catalyst 8510CSR, 8510MSR, 8540CSR, and 8540MSR series.
- Cisco 10000 ESR and 12000 GSR series.
- LS1010 and Cisco 6260–NI2.
- DistributedDirector (except that igs-w3 images are not vulnerable).

Products Confirmed Not Vulnerable

Cisco products that are not affected by this vulnerability either because they have no support for ATM and ILMI, or because they do not run IOS include, but are not limited to:

- Catalyst ATM blade (runs possibly affected code, but an SNMP connection to the blade is not possible).
- Cisco 800 and 805 series.
- Cisco Universal Broadband Routers ubr900 and ubr920.
- Cisco 1003, 1004, and 1005 series.
- Cisco 1600, 2500, 2800, 4000 series.
- Cisco 2500 Fixed Frad.
- Cisco 3800 (not to be confused with MC3810).
- Cisco 5100, 5200, and 5300 series access servers.
- Catalyst 6000 Supervisor Module.
- Cisco PIX Firewall.
- Aironet and Cisco/Aironet wireless products.
- CS11000, Cache Engine, LocalDirector, and network scaling products (except that the Distributed Director might be affected).
- VPN products such as Altiga concentrators.
- Host-based network management or access management products.
- Cisco IP Telephony and telephony management software (except those that are hosted on a vulnerable IOS platform).
- Voice gateways and convergence platforms (except those that are hosted on a vulnerable IOS platform).
- Optical switch products such as the ONS 15000 series.

No other Cisco products are currently known to be affected by these vulnerabilities.

Details

ILMI (Interim Local Management Interface) is an independent industry standard used for configuration of ATM (Asynchronous Transfer Mode) interfaces. The standard specifies the use of mechanisms and formats previously defined by SNMP (Simple Network Management Protocol). Although it is based on SNMP, ILMI communication actually occurs using a transport other than IP (Internet Protocol) that traverses only the physical ATM link. ILMI is essential to functions such as ATM auto-discovery and LANE (LAN Emulation).

SNMP "objects" are variables that are organized into a MIB (Management Information Base). The MIB has a tree structure and contains both operational (read-only) data as well as configuration (read-write) options. By specifying a community string of "ILMI" in an SNMP request, access can be obtained to read the objects in three specific parts of the overall management tree structure on any device affected by this vulnerability: the MIB-II system group, the LAN-EMULATION-CLIENT MIB, and the PNNI (Private Network-to-Network Interface) MIB. A subset of objects in each part can be modified using the same "ILMI" community string.

Cisco Security Advisory: Cisco IOS Software SNMP Read-Write ILMI Community String Vulnerability

The MIB-II system group contains basic information about the device itself. The number of objects that can be modified is limited. Examples include:

- **system.sysContact** — The contact information for the person or organization responsible for managing the device.
- **system.sysLocation** — A description of the physical location where the device is installed or operating.
- **system.sysName** — The hostname of the device, how it identifies itself at the console prompt. (This might not be the same name by which the device is known to other hosts on the network.)

Most of the objects in the system MIB are read-only and cannot be changed via SNMP, such as the time elapsed since the previous restart and textual descriptions of the device's hardware and software.

Numerous objects can be viewed in the LAN-EMULATION-CLIENT MIB and PNNI MIB, and modification of some of the read-write objects can have an affect on ATM operation of the device. The objects in the LAN-EMULATION-CLIENT MIB can only be viewed or modified if LANE has already been configured on the device.

Access to SNMP in Cisco IOS software can be limited by applying access control lists (ACLs), by modifying or removing the SNMP view, by removing the community string from the running configuration, or by disabling the SNMP service. Any SNMP query that does not meet the criteria for access is promptly discarded when such protective measures are in place. If a query does meet the criteria for access, then a response is formulated and sent.

It is possible to configure the device so that the ILMI community string is unavailable in all IOS 11.1 and higher releases. The particular method selected to accomplish this depends on the specific IOS release and configuration.

This defect is documented as CSCdp11863. The vulnerability is repaired by imposing a test such that an SNMP request using the "ILMI" community string will only be recognized if it has been transported by ILMI.

ATM functionality was added in various 10.x releases of Cisco IOS software. However, the function containing the defect was introduced when support for ILMI and other ATM features was added in IOS release 11.0(0.2). Therefore, all prior releases are not vulnerable.

A separate Cisco Security Advisory has been announced regarding additional SNMP vulnerabilities. That advisory, <http://www.cisco.com/warp/public/707/ios-snmpp-community-vulns-pub.shtml>, should be consulted in tandem with this notice.

Impact

If SNMP requests can be received by an affected device, then certain MIB objects can be viewed without proper authorization, causing a violation of confidentiality.

A subset of the readable MIB objects can be modified without authorization to cause a failure of integrity. For example, the hostname can be modified so as to confuse network administrators, or the contact and location information could be changed with a goal of disrupting operations or embarrassing whoever is responsible for the device.

Objects in the LAN-EMULATION-CLIENT and PNNI MIBs can be viewed and modified, thus resulting in changes to the operation of ATM functions. If ATM is in use on the device, this may result in a failure of availability.

Cisco Security Advisory: Cisco IOS Software SNMP Read-Write ILMI Community String Vulnerability

Any affected device that is not otherwise protected against the receipt of SNMP packets is vulnerable to a denial-of-service (DoS) attack by flooding the SNMP port with read or write requests.

Software Versions and Fixes

The following table summarizes the known affected Cisco IOS software releases and the earliest estimated dates of availability for fixed releases. All dates are tentative and subject to change.

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

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 defect. Although it receives less testing, it contains only the minimal changes necessary to effect the repair.
- **Interim** – Built at regular intervals between maintenance releases and receive less testing. Interims should be selected only if there is no other suitable release that addresses the vulnerability. Interim releases are usually not available for customer download via CCO without prior arrangement.

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 following section.

More information on IOS release names and abbreviations is available at <http://www.cisco.com/warp/public/620/1.html>.

Train	Description of Image or Platform	Availability of Fixed Releases*		
11.x-based Releases		Rebuild	Interim**	Maintenance
10.3 and earlier	All	Not Affected		
11.0-based Releases		Rebuild	Interim**	Maintenance
11.0	Major GD release for all platforms	11.0(22a)		
		2001-Mar-19		
11.1-based Releases		Rebuild	Interim**	Maintenance
11,1	Major release for all platforms	11.1(24a)		
		2001-Mar-19		
11.1AA	ED release for access servers: 1600, 3200, and 5200 series.			12.1(7)
11.1CA	Platform-specific support for 7500,	11.1(36)CA1		2001-Feb-26

	7200, 7000, and RSP	2001-Mar-02		
11.1CC	ISP train: added support for FIB, CEF, and NetFlow on 7500, 7200, 7000, and RSP	11.1(36)CC1		
11.1CT	Added support for Tag Switching on 7500, 7200, 7000, and RSP	2001-Mar-02 12.0(11)ST2		
11.1IA	DistributedDirector only	2001-Feb-26 11.1(28)IA1		
11.2-based Releases		2001-Mar-02		
		Rebuild	Interim**	Maintenance
11.2	Major release, general deployment	11.2(25a)		
11.2BC	Platform-specific support for IBM networking, CIP, and TN3270 on 7500, 7000, and RSP	2001-Mar-05		12.1(7)
11.2GS	Early deployment release to support 12000 GSR	12.0(15)S1		2001-Feb-26
11.2P	New platform support	2001-Feb-20 11.2(25a)P		
		2001-Mar-05		
11.2SA	Catalyst 2900XL switch only			12.0(5)WC
				2001-Apr-12
11.2WA3	LS1010 ATM switch		12.0(10)W(18b)	12.0(13)W5(19b)
			Available	Available
11.2(4)XA	Initial release for the 1600 and 3600	11.2(25a)P		
		2001-Mar-05		
11.2(9)XA	Initial release for the 5300 and digital modem support for the 3600	11.2(25a)P		
11.3-based Releases		2001-Mar-5		
		Rebuild	Interim**	Maintenance
11.3	Major release for all platforms	2001-Mar-05		
		2001-Mar-05		

11.3AA	ED for dial platforms and access servers: 5800, 5200, 5300, 7200	11.3(11a)AA		
11.3DA	Early deployment train for ISP DSLAM 6200 platform	2001-Mar-05 12.1(5)DA1		
11.3DB	Early deployment train for ISP/Telco/PTT xDSL broadband concentrator platform, (NRP) for 6400	2001-Mar-19 12.1(4)DB1		
11.3HA	Short-lived ED release for ISR 3300 (SONET/SDH router)	2001-Feb-27 Not Vulnerable		
11.3MA	MC3810 functionality only	11.3(1)MA8		
11.3NA	Voice over IP, media convergence, various platforms	2001-Mar-19 12.1(7)		
11.3T	Early deployment major release, feature-rich for early adopters	2001-Mar-05 11.3(11b)T1		
11.3WA4	Multilayer Switching and Multiprotocol over ATM functionality for LS1010	2001-Mar-05	12.0(10)W(18b)	12.0(13)W5(19b)
	Introduction ofubr7246 and 2600	11.3(11b)T1	Available	Available
12.0-based Releases		2001-Mar-05 Rebuild	Interim**	Maintenance
12.0	General deployment release for all platforms		12.0(7.1)	12.0(8)
12.0DA	xDSL support: 6100, 6200		Available 12.0(7.1)T	Available
12.0DB		12.1(4)DB1	Available	

	ISP/Telco/PTT xDSL broadband concentrator platforms	2001-Feb-26		
12.0DC	6400 Access Concentrator	12.1(4)DC2		
		2001-Feb-26		
12.0S	Core/ISP support: GSR, RSP, c7200	12.0(15)S1		
		2001-Feb-20		
12.0SC	Cable/broadband ISP: ubr7200			12.0(15)SC
				2001-Mar-05
12.0SL	10000 ESR: c10k	12.0(14)SL1		
		2001-Feb-26		
12.0ST	General deployment release for all platforms	12.0(11)ST2		
12.0T	Early Deployment(ED): VPN, Distributed Director, various platforms	2001-Feb-26		12.1(7)
12.0W5	cat8510c, ls1010, cat8510m			2001-Feb-26 12.0(10)W5(18c)
				Available
	cat8540c, cat8540m			12.0(10)W5(18b)
				Available
	cat5atm, c6msm			12.0(13)W5(19)
				Available
	cat2948g-L3			12.0(10)W5(18e)
			Available	
	cat4232			12.0(10)W5(18f)
				Available
	cat4840g			12.0(10)W5(18)
				Available
12.0WT	cat4840g			12.0(13)WT6(1)
				2001-Mar-15
12.0XA	Early Deployment (ED): limited platforms			12.1(7)
12.0XB	Short-lived early deployment release			2001-Feb-26 12.1(7)
				2001-Feb-26

12.0XC	Early Deployment (ED): limited platforms			12.1(7)
12.0XD	Early Deployment (ED): limited platforms			2001-Feb-26 12.1(7)
12.0XE	Early Deployment (ED): limited platforms	12.1(5c)E8		2001-Feb-26
12.0XF	Early Deployment (ED): limited platforms	2001-Mar-5		12.1(7)
12.0XG	Early Deployment (ED): limited platforms			2001-Feb-26 12.1(7)
12.0XH	Early Deployment (ED): limited platforms	12.0(4)XH5		2001-Feb-26
12.0XI	Early Deployment (ED): limited platforms	2001-Mar-12		12.1(7)
12.0XJ	Early Deployment (ED): limited platforms			2001-Feb-26 12.1(7)
12.0XK	Early Deployment (ED): limited platforms	12.0(7)XK4		2001-Feb-26
12.0XL	Early Deployment (ED): limited platforms	2001-Mar-26 12.0(4)XH5		
12.0XM	Short-lived early deployment release	2001-Mar-12		12.1(7) 2001-Feb-26
12.0XN	Early Deployment (ED): limited platforms			
12.0XP	Early Deployment (ED): limited platforms	Not Vulnerable		
12.0XQ	Short-lived early deployment release			12.1(7) 2001-Feb-26
12.0XR	Short-lived early deployment release	12.1(5)T5		
12.0XS		2001-Mar-05 12.1(5c)E8		

	Short-lived early deployment release	2001-Mar-5		
12.0XU	Early Deployment (ED): limited platforms	Not Vulnerable		
12.0XV	Short-lived early deployment release	12.1(5)T5		
		2001-Mar-05		
12.0XW	Early Deployment (ED): limited platforms	Not Vulnerable		
12.1-based and Later Releases		Rebuild	Interim**	Maintenance
All 12.1 Releases	Various platforms	Not Vulnerable		
Notes				
* 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.				

Workarounds

Several workarounds are available based on customer needs, equipment, and software features. The usefulness and practicality of each workaround depends on the IOS release running on the device and many variables in the customer's environment. Customers are urged to consider each of the following alternatives carefully before deploying. These workarounds are only needed if it is not possible to upgrade to an unaffected release of IOS software.

1. Default workaround for use with releases for which no other workarounds are effective:
 - a. Applying access lists to all the interfaces of the vulnerable device blocking SNMP from all hosts but those authorized to manage the devices.
 - b. Blocking SNMP access at the edge of the network to prevent undesirable SNMP traffic from entering the network containing the vulnerable device.

Access lists should be deployed with careful consideration of the possible effects on network operation and performance. Also note that authentication based on an IP source address is weak, so the preceding method will not protect against certain types of attacks in which the IP source address has been spoofed. Further information can be found in the Cisco document "Improving Security on Cisco Routers", available at <http://www.cisco.com/warp/public/707/21.html>
2. For affected releases based on IOS 11.1:
 - a. Remove the view so that the ILMI community cannot be reached:
no snmp-server view *ilmi
 - b. This configuration will not survive a system reload. The command must be re-entered after every restart of the system.
3. For affected releases of IOS 11.2 through 11.3(8) **NOT REQUIRING ATM:**
In this affected range of releases, the ILMI community string can be modified or deleted. However, the changes will not persist through a reboot of the device. These instructions must be reapplied following every system reload of the affected device:

- a. Expose the undocumented ILMI community string so it can be modified:
snmp-server community ILMI RW
The preceding command may cause an error that can be safely ignored.
- b. Disable read-write capability for the same community:
no snmp-server community ILMI RW
If an error is displayed, then this workaround cannot be applied to the device. Use the default workarounds presented in the first item above.
- c. Since this configuration will not survive a system reload, the command must be reentered after every restart of the system.

If the command in item 2 above did not generate an error and ATM is not needed on this device, then this workaround is complete.

4. For affected releases of IOS 11.2 through 11.3(8) **THAT REQUIRE ATM:**

Note: This workaround is not valid for ATM switches such as the LS1010 and 8500 series. See section I for those devices.

This workaround will allow ILMI to continue to function for ATM while constraining who may reconfigure the device by way of the ILMI community string:

- a. Create a simple ACL to deny access using the following command. If "66" is already in use, choose a different two-digit number:
access-list 66 deny any
- b. Apply it generally to the ILMI community to restrict its view:
snmp community ILMI view *ilmi RW 66
An error will be reported if the *ilmi view doesn't exist. If that occurs, then use the following command to explicitly restrict the ILMI view:
snmp community ILMI RW 66
If the preceding command produces persistent errors, then this workaround cannot be applied to this device. Use the default workarounds presented in the first item above.

5. For affected releases of IOS 11.3(9) through 12.0(2)T **NOT REQUIRING ATM:**

All versions of IOS in this range will accept this workaround. However, the changes will not persist through a reboot of the device. These instructions must be reapplied following every system reload of the affected device:

- a. Expose the undocumented ILMI community string so it can be modified:
snmp-server community ILMI RW
The preceding command may cause an error that can be safely ignored.
- b. Disable read-write capability for the same community:
no snmp-server community ILMI RW
If an error is displayed, then this workaround cannot be applied to the device. Stop this procedure and use the default workarounds presented in the first item above.
- c. This configuration will not survive a system reload. The command must be reentered after every restart of the system.

6. For affected releases of IOS 11.3(9) through 12.0(2)T **THAT REQUIRE ATM:**

Note: This workaround is not valid for ATM switches such as the LS1010 and 8500 series. This workaround is also not valid for 12.0 releases that are based on 12.0(3)T and higher such as 12.0S. See section I for those devices.

This workaround will allow ILMI to continue to function for ATM while constraining who may reconfigure the device by way of the ILMI community string:

- a. Create a simple ACL to deny access using the following command. If "66" is already in use,

choose a different two-digit number:

access-list 66 deny any

- b. Apply it generally to the ILMI community to restrict its view:

snmp community ILMI view *ilmi RW 66

An error will be reported if the *ilmi view doesn't exist. If that occurs, then use the following command to explicitly restrict the ILMI view:

snmp community ILMI RW 66

If the preceding command produces persistent errors, then this workaround cannot be applied to this device. Use the default workaround presented in the first item above.

7. For affected releases of IOS 12.0(3)T and later:

These releases of IOS include support for Simple Network Management Protocol version 3 (SNMPv3), which is required for this workaround.

Confirm the presence of SNMPv3 support by asking the console CLI (command-line interpreter) for assistance with options to complete the **snmp-server** command. Enter config mode, enter the command shown below, and note the expected response:

snmp-server user test test ?

```
remote Specify a remote SNMP entity to which the user belongs
v1      user using the v1 security model
v2c     user using the v2c security model
v3      user using the v3 security model
```

If the preceding command did not produce the expected results, then SNMPv3 is not supported in the release and this workaround cannot be applied. Stop this procedure and consider applying the default workaround presented above in the first item.

Otherwise, if the device responded as expected, continue with the following explanation and instructions.

In these IOS releases (12.0(3)T and later), ILMI packets are processed by the SNMP engine in the same manner as ordinary IP SNMP packets. An access control list or a view applied to the ILMI community string will be processed whether the transport is ILMI or IP. However, the only types of access control lists that can be applied to a community string are via IP access-list statements, which when applied, block ALL non-IP packets, including ILMI packets. Modifying or deleting the *ilmi view will also affect the packets transported by ILMI, so workarounds that change the view are equally ineffective at permitting ILMI while denying SNMP. **In this range of releases, it is not possible to apply a workaround that denies IP SNMP packets that does not also deny ILMI SNMP packets.**

8. For affected releases of IOS 12.0(3)T and later **NOT REQUIRING ATM:**

- a. Expose the undocumented ILMI community string so it can be modified:

snmp-server community ILMI RW

The preceding command may cause an error that can be safely ignored.

- b. Disable read-write capability for the same community:

no snmp-server community ILMI RW

If an error is displayed, then this workaround cannot be applied to the device. Stop this procedure and consider using the default workaround.

9. For affected releases of IOS 12.0(3)T and later **THAT REQUIRE ATM:**

Note: This section also applies to ATM switch software such as for the LS1010 and the 8500 series. This section also applies to other 12.0 releases that are based on 12.0(3)T and higher such as 12.0S.

The **only** effective workaround for systems in this category is the default workaround:

- a. Applying access lists to all the interfaces of the vulnerable device blocking SNMP from all

hosts but those authorized to manage the devices.

- b. Blocking SNMP access at the edge of the network to prevent undesirable SNMP traffic from entering the network containing the vulnerable device.

Access lists should be deployed with careful consideration of the possible effects on network operation and performance. Also note that authentication based on an IP source address is weak, so the preceding method will not protect against certain types of attacks in which the IP source address has been spoofed.

In this range of releases it is not possible to block IP SNMP packets while permitting ILMI SNMP packets. The alternative workarounds presented previously will almost certainly cause a failure of ATM ILMI communications resulting in a loss of ATM connectivity, either immediately upon configuration, or unexpectedly at some later time. Either use the default workaround or upgrade to fixed software.

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@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

This vulnerability is known to the engineering staff of several Cisco customers. Cisco considers it known to the public prior to the publication of this notice.

Cisco is aware of one recent incident involving the unauthorized modification of a router that appears to have resulted from this vulnerability. However, it may have been the unintended side-effect of a test of the vulnerability.

Cisco is not aware of any available tools specifically designed to make use of this vulnerability. However, various off-the-shelf network management programs could easily be used to test for this vulnerability and to exploit it. Certain widely-available programs known to the cracker community could be modified by any reasonably competent programmer to automate the abuse of this vulnerability.

Cisco is not aware of any general public discussion of this vulnerability other than the exceptions previously noted.

Status of This Notice: INTERIM

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. CISCO EXPECTS TO UPDATE THIS DOCUMENT AS NEW INFORMATION BECOMES AVAILABLE.

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 notice will be posted at
<http://www.cisco.com/warp/public/707/cisco-sa-20010227-ios-snmp-ilmi.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
- bugtraq@securityfocus.com
- firewalls@lists.gnac.com

- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- comp.dcom.sys.cisco
- firewalls@lists.gnac.com
- Various internal Cisco mailing lists

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

Revision History

Revision 1.5	2001-March-07	Corrected fixed release versions in table
Revision 1.4	2001-March-02	Corrected fixed release versions in table
Revision 1.3	2001-February-28	Corrected fixed release versions in table, modified workarounds for clarity
Revision 1.2	2001-February-27	Error corrected in Affected Products
Revision 1.1	2001-February-27	Error corrected in Workaround
Revision 1.0	2001-February-27	First interim public version

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 Web site at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices.

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Mar 07, 2001

Document ID: 13630
