

# Cisco Security Advisory: IOS HTTP Authorization Vulnerability

Document ID: 13626

Advisory ID: cisco-sa-20010627-ios-http-level

<http://www.cisco.com/warp/public/707/cisco-sa-20010627-ios-http-level.shtml>

## Revision 1.8

Last Updated 2003 September 23 0800 UTC (GMT)

For Public Release 2001 June 27 1500 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: FINAL](#)  
[Distribution](#)  
[Revision History](#)  
[Cisco Security Procedures](#)

---

## Summary

When the HTTP server is enabled and local authorization is used, it is possible, under some circumstances, to bypass the authentication and execute any command on the device. In that case, the user will be able to exercise complete control over the device. All commands will be executed with the highest privilege (level 15).

All releases of Cisco IOS® software, starting with release 11.3 and later, are vulnerable. Virtually all mainstream Cisco routers and switches running Cisco IOS software are affected by this vulnerability.

Products that are not running Cisco IOS software are not vulnerable.

The workaround for this vulnerability is to disable HTTP server on the router or to use Terminal Access Controller Access Control System (TACACS+) or Radius for authentication.

This advisory will be posted at  
<http://www.cisco.com/warp/public/707/cisco-sa-20010627-ios-http-level.shtml>.

# Affected Products

This section provides details on affected products.

## Vulnerable Products

Any device running Cisco IOS software release 11.3 and later is vulnerable.

Cisco devices that may be running with affected Cisco IOS software releases include but are not limited to:

- Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 800, ubr900, 1000, 1400, 1500, 1600, 1700, 2500, 2600, 3000, 3600, 3800, 4000, 4500, 4700, AS5200, AS5300, AS5800, 6400, 7000, 7100, 7200, ubr7200, 7500, and 12000 series.
- Most recent versions of the LS1010 ATM switch.
- The Catalyst 6000 and 5000 if they are running Cisco IOS software.
- The Catalyst 2900XL and 3500XL LAN switch only if it is running Cisco IOS software.
- The Catalyst 2900 and 3000 series LAN switches are affected.
- The Cisco Distributed Director.

For some products, the affected software releases are relatively new and may not be available on every device listed above.

## Products Confirmed Not Vulnerable

*If you are not running Cisco IOS software, you are not affected by this vulnerability.*

Cisco products that do not run Cisco IOS software and are not affected by this defect include, but are not limited to:

- 700 series dial-up routers (750, 760, and 770 series).
- The Catalyst 6000 and 5000 are not affected if they are not running Cisco IOS software.
- WAN switching products in the IGX and BPX lines.
- The MGX (formerly known as the AXIS shelf).
- Host-based software.
- The Cisco PIX Firewall.
- The Cisco Local Director.
- The Cisco Cache Engine.

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

## Details

By sending a crafted URL it is possible to bypass authentication and execute any command on the router at level 15 (enable level, the most privileged level). This will happen only if the user is using a local database for authentication (usernames and passwords are defined on the device itself). The same URL will not be effective against every Cisco IOS software release and hardware combination. However, there are only 84 different combinations to try, so it would be easy for an attacker to test them all in a short period of time.

The URL in question follows this format:

```
http://<device_address>/level/xx/exec/...
```

Where **xxx** is a number between 16 and 99.

This vulnerability is documented as Cisco Bug ID **CSCdt93862**.

## Impact

An attacker can exercise complete control over the device. By exploiting this vulnerability, the attacker can see and change the configuration of the device.

## 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. 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 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 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 via manufacturing, and usually they are not available for customer download from CCO without prior arrangement with the Cisco 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 following section.

More information on Cisco IOS software 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* |           |             |
|---------------------------------|----------------------------------|---------------------------------|-----------|-------------|
| 11.0-based Releases and Earlier |                                  | Rebuild                         | Interim** | Maintenance |
| 10.3                            | Multiple releases and platforms  | Not affected                    |           |             |
| 11.0                            | Multiple releases and platforms  | Not affected                    |           |             |
| 11.1-based Releases             |                                  | Rebuild                         | Interim** | Maintenance |

|                     |   |   |           |             |
|---------------------|---|---|-----------|-------------|
| 11.1                | Major release for all platforms   | Not affected  |           |             |
| 11.2–based Releases |   | Rebuild   | Interim** | Maintenance |
| 11.2                | Major release for all platforms   | End of Engineering                                      |           |             |
| 11.3–based Releases |   | Rebuild   | Interim** | Maintenance |
| 11.3                | Major release for all platforms   | End of Engineering                                      |           |             |
|                     |   | Upgrade recommended to 12.0(18)                         |           |             |
| 11.3AA              | ED for dial platforms and access servers: 5800, 5200, 5300, 7200                              | Not Scheduled   |           |             |
| 11.3DA              | Early deployment train for ISP DSLAM 6200 platform  | Upgrade recommended to 12.1(9)<br>End of Engineering    |           |             |
| 11.3DB              | Early deployment train for ISP/Telco/PTT xDSL broadband concentrator platform, (NRP) for 6400 | Upgrade recommended to 12.1(7)DA2<br>End of Engineering |           |             |
| 11.3HA              | Short–lived ED release for ISR 3300 (SONET/SDH router)  | Upgrade recommended to 12.1(5)DB2<br>End of Engineering |           |             |
| 11.3MA              | MC3810 functionality only   | Upgrade recommended to 12.0(18)<br>End of Engineering   |           |             |
|                     |   | Upgrade recommended to 12.1(9)                          |           |             |
| 11.3NA              | Voice over IP, media convergence, various platforms   | End of Engineering                                      |           |             |
| 11.3T               | Early deployment major release, feature–rich for early adopters                               | Upgrade recommended to 12.1(9)<br>End of Engineering    |           |             |
| 11.3XA              | Introduction ofubr7246 and 2600   | Upgrade recommended to 12.0(18)<br>End of Engineering   |           |             |
|                     |   | Upgrade recommended to 12.0(18)                         |           |             |
| 11.3WA4             | LightStream 1010  | End of Engineering                                      |           |             |
|                     |   | Upgrade recommended to 12.0W                            |           |             |

| 12.0-based Releases |   | Rebuild                           | Interim** | Maintenance                   |
|---------------------|---|-----------------------------------|-----------|-------------------------------|
| 12.0                | General Deployment release for all platforms  |                                   |           | 12.0(18)                      |
| 12.0DA              | xDSL support: 6100, 6200  | Not Scheduled                     |           |                               |
|                     |   | Upgrade recommended to 12.1(7)DA2 |           |                               |
| 12.0DB              | Early Deployment (ED) release, which delivers support for the Cisco 6400 Universal Access Concentrator (UAC) for Node Switch Processor (NSP).                       | Not Scheduled                     |           |                               |
|                     |   | Upgrade recommended to 12.1(5)DB2 |           |                               |
| 12.0DC              | Early Deployment (ED) release, which delivers support for the Cisco 6400 Universal Access Concentrator (UAC) for Node Switch Processor (NSP).                       | Not Scheduled                     |           |                               |
| 12.0S               | Core/ISP support: GSR, RSP, c7200   | Upgrade recommended to 12.1DC     |           | 12.0(18)S Available 2001-July |
| 12.0SC              | Cable/broadband ISP: ubr7200  | 12.0(16)SC                        |           |                               |
| 12.0SL              | 10000 ESR: c10k   | Not affected                      |           |                               |
| 12.0ST              | Cisco IOS software Release 12.0ST is an early deployment (ED) release for the Cisco 7200, 7500/7000RSP and 12000 (GSR) series routers for Service Providers (ISPs). |                                   |           | 12.0(18)ST 2001-Jul-02        |
| 12.0T               | Early Deployment(ED): VPN, Distributed  | Not Scheduled                     |           |                               |
|                     |   | Upgrade recommended to 12.1(9)    |           |                               |

|                 |  |                                  |                           |                                   |
|-----------------|--|----------------------------------|---------------------------|-----------------------------------|
|                 | Director, various platforms  |                                  |                           |                                   |
| 12.0(13)W5(19c) | Catalyst switches: cat8510c, cat8540c, c6msm, ls1010, cat8510m, cat8540m | Not vulnerable                   |                           |                                   |
| 12.0(10)W5(18g) | Catalyst switches: cat2948g, cat4232                                     |                                  |                           | 12.0(18)W5(22a)<br>2001–August–23 |
| 12.0(14)W5(20)  | Catalyst switches: cat5000ATM  |                                  |                           | 12.0(18)W5(22)<br>2001–August–03  |
| 12.0WC          |  |                                  | 12.0(5.4)WC1<br>2001–July |                                   |
| 12.0WT          | cat4840g   | Not Scheduled                    |                           |                                   |
|                 |  | Upgrade to be determined         |                           |                                   |
| 12.0XA          | Early Deployment (ED): limited platforms                                 | Not Scheduled                    |                           |                                   |
|                 |  |                                  |                           |                                   |
| 12.0XB          | Short-lived early deployment release                                     | Upgrade recommended to 12.1(9)   |                           |                                   |
|                 |  | Not Scheduled                    |                           |                                   |
| 12.0XC          | Early Deployment (ED): limited platforms                                 | Upgrade recommended to 12.1(9)   |                           |                                   |
|                 |  | Not Scheduled                    |                           |                                   |
| 12.0XD          | Early Deployment (ED): limited platforms                                 | Upgrade recommended to 12.1(9)   |                           |                                   |
|                 |  | Not Scheduled                    |                           |                                   |
| 12.0XE          | Early Deployment (ED): limited platforms                                 | Upgrade recommended to 12.1(9)   |                           |                                   |
|                 |  | Not Scheduled                    |                           |                                   |
| 12.0XF          | Early Deployment (ED): limited platforms                                 | Upgrade recommended to 12.1(8a)E |                           |                                   |
|                 |  | Not Scheduled                    |                           |                                   |
| 12.0XG          | Early Deployment (ED): limited platforms                                 | Upgrade recommended to 12.1(9)   |                           |                                   |
|                 |  | Not Scheduled                    |                           |                                   |
| 12.0XH          | Early Deployment (ED): limited platforms                                 | Upgrade recommended to 12.1(9)   |                           |                                   |
|                 |  | Not Scheduled                    |                           |                                   |
| 12.0XI          | Early Deployment (ED): limited platforms                                 | Upgrade recommended to 12.1(9)   |                           |                                   |
|                 |  | Not Scheduled                    |                           |                                   |
| 12.0XJ          | Early Deployment (ED): limited   | Upgrade recommended to 12.1(9)   |                           |                                   |
|                 |  | Not Scheduled                    |                           |                                   |
|                 |  | Upgrade recommended to 12.1(9)   |                           |                                   |

|                     |  |   |             |             |
|---------------------|--|---|-------------|-------------|
|                     | platforms                                |   |             |             |
| 12.0(5)XK           | Early Deployment (ED): limited platforms | Not Scheduled   |             |             |
| 12.0(7)XK           | Early Deployment (ED): limited platforms | Upgrade recommended to 12.1(9)<br>Not Scheduled       |             |             |
| 12.0XL              | Early Deployment (ED): limited platforms | Upgrade recommended to 12.1(9)<br>Not Scheduled       |             |             |
| 12.0XM              | Early Deployment (ED): limited platforms | Upgrade recommended to 12.1(9)<br>Not Scheduled       |             |             |
| 12.0XN              | Early Deployment (ED): limited platforms | Availability date to be determined<br>Not Scheduled   |             |             |
| 12.0XP              | Early Deployment (ED): limited platforms | Upgrade recommended to 12.1(9)<br>Not Scheduled       |             |             |
| 12.0XQ              | Early Deployment (ED): limited platforms | Upgrade recommended to 12.0(5.4)WC1<br>Not Scheduled  |             |             |
| 12.0XR              | Early Deployment (ED): limited platforms | Upgrade recommended to 12.1(9)<br>Not Scheduled       |             |             |
| 12.0XS              | Early Deployment (ED): limited platforms | Upgrade recommended to 12.2(1b)<br>End of Engineering |             |             |
| 12.0XU              | Early Deployment (ED): limited platforms | Upgrade recommended to 12.1(8a)E<br>Not Scheduled     |             |             |
| 12.0XV              | Early Deployment (ED): limited platforms | Upgrade recommended to 12.0(5.4)WC1<br>Not Scheduled  |             |             |
| 12.1-based Releases |  | Upgrade recommended to 12.2(1b)                       | 2001-Jul-02 |             |
|                     |  | Rebuild   | Interim**   | Maintenance |
| 12.1                | LD release for all platforms             |   |             | 12.1(9)     |
| 12.1AA              | Dial support                             |   |             | 12.1(9)AA   |
| 12.1CX              | Core/ISP support: GSR, RSP, c7200        |   |             |             |
| 12.1DA              | xDSL support: 6100, 6200                 | 12.1(7)DA2<br>2001-Jun-18                             |             |             |
| 12.1DB              |  |   |             |             |

|        |   |  |              |                          |
|--------|---|--|--------------|--------------------------|
|        | Cisco IOS Software Release 12.1(1)DB supports Cisco's 6400 Universal Access Concentrator  |  |              |                          |
| 12.1DC | Cisco IOS Software Release 12.1(1)DC supports Cisco's 6400 Universal Access Concentrator  |  |              |                          |
| 12.1E  | Core/ISP support: GSR, RSP, c7200   |  |              | 12.1(8a)E<br>2001-Jul-09 |
| 12.1EC | 12.1EC is being offered to allow early support of new features on the uBR7200 platform, as well as future support for new Universal Broadband Router headend platforms. |  | 12.1(6.5)EC3 |                          |
| 12.1EX | Catalyst 6000 support   |  |              | 12.1(8a)E<br>2001-Jul-09 |
| 12.1EY | Cat8510c, Cat8510m, Cat8540c, Cat8540m, LS1010  |  |              | 12.1(6)EY                |
| 12.1EZ | Early Deployment (ED): special image  | 12.1(6)EZ1                                       |              |                          |
| 12.1T  | Early Deployment(ED): VPN, Distributed Director, various platforms  | Not Scheduled                                    |              |                          |
|        |   |  |              |                          |
| 12.1XA | Early Deployment (ED): limited platforms  | Upgrade recommended to 12.2(1b)<br>Not Scheduled |              |                          |
|        |   |  |              |                          |
| 12.1XB | Early Deployment (ED): limited platforms  | Upgrade recommended to 12.2(1b)                  |              |                          |

|        |  |                                   |  |                                 |
|--------|--|-----------------------------------|--|---------------------------------|
| 12.1XC | Early Deployment (ED): limited platforms         |                                   |  | 12.1(9)AA                       |
| 12.1XD | Early Deployment (ED): limited platforms         | Not Scheduled                     |  |                                 |
|        |  |                                   |  |                                 |
| 12.1XE | Early Deployment (ED): limited platforms         | Upgrade recommended to 12.2(1b)   |  |                                 |
| 12.1XF | Early Deployment (ED): 811 and 813 (c800 images) | 12.1(2)XF4<br>2001–July–09        |  |                                 |
| 12.1XG | Early Deployment (ED): 800, 805, 820, and 1600   | 12.1(5)XG5<br>2001–July–09        |  |                                 |
| 12.1XH | Early Deployment (ED): limited platforms         | Not Scheduled                     |  |                                 |
|        |  |                                   |  |                                 |
| 12.1XI | Early Deployment (ED): limited platforms         | Upgrade recommended to 12.2(1b)   |  |                                 |
|        |  | Not Scheduled                     |  |                                 |
| 12.1XJ | Early Deployment (ED): limited platforms         | Upgrade recommended to 12.2(1b)   |  |                                 |
|        |  | Not Scheduled                     |  |                                 |
| 12.1XK | Early Deployment (ED): limited platforms         | Upgrade recommended to 12.1(3)YB4 |  |                                 |
| 12.1XL | Early Deployment (ED): limited platforms         | Not Scheduled                     |  |                                 |
|        |  |                                   |  |                                 |
| 12.1XM | Short-lived early deployment release             | 12.1(4)XM4<br>2001–June–27        |  | Upgrade recommended to 12.2(1b) |
| 12.1XP | Early Deployment (ED): 1700 and SOHO             | 12.1(3)XP4                        |  |                                 |
| 12.1XQ | Short-lived early deployment release             | Not Scheduled                     |  |                                 |
|        |  |                                   |  |                                 |
| 12.1XR | Short-lived early deployment release             | 12.1(5)XR2                        |  | Upgrade recommended to 12.2(1b) |
| 12.1XS | Short-lived early deployment release             | 12.1(5)XS2<br>2001–July           |  |                                 |

|                     |  |                                   |            |                           |
|---------------------|--|-----------------------------------|------------|---------------------------|
| 12.1XT              | Early Deployment (ED): 1700 series           | 12.1(3)XT3                        |            |                           |
| 12.1XU              | Early Deployment (ED): limited platforms     | 12.1(5)XU1                        |            |                           |
| 12.1XV              | Short-lived early deployment release         | 12.1(5)XV3<br>2001–July           |            |                           |
| 12.1XW              | Short-lived early deployment release         | Not Scheduled                     |            |                           |
|                     |  |                                   |            |                           |
| 12.1XX              | Short-lived early deployment release         | Upgrade recommended to 12.2DD     |            | 12.1(6)EZ                 |
| 12.1XY              | Short-lived early deployment release         | 12.1(5)XY6<br>2001–July           |            |                           |
| 12.1XZ              | Short-lived early deployment release         | 12.1(5)XZ4<br>2001–July           |            |                           |
| 12.1YA              | Short-lived early deployment release         | Not Scheduled                     |            |                           |
|                     |  | Upgrade recommended to 12.2(2)XB  |            |                           |
| 12.1YB              | Short-lived early deployment release         | 2001–August<br>12.1(5)YB4         |            |                           |
| 12.1YC              | Short-lived early deployment release         | 12.1(5)YC1                        |            |                           |
| 12.1YD              | Short-lived early deployment release         | 12.1(5)YD2<br>2001–June–25        |            |                           |
| 12.1YF              | Short-lived early deployment release         | 12.1(5)YF2                        |            |                           |
| 12.2-based Releases |  | Rebuild                           | Interim**  | Maintenance               |
| 12.2                | LD release for all platforms                 | 12.2(1b) <sup>1</sup><br>12.2(1c) | 12.2(1.1)  | 12.2(3)<br>2001–August    |
| 12.2T               | General deployment release for all platforms |                                   | 12.2(2.2)T |                           |
| 12.2XA              | SPLOB  |                                   |            | 12.2(2)XA<br>2001–July–02 |

|  |                                      |            |  |                           |
|--|--------------------------------------|------------|--|---------------------------|
| 12.2XD   | Short-lived early deployment release | 12.2(1)XD1 |  |                           |
| 12.2XE   | Short-lived early deployment release |            |  | 12.2(1)XE                 |
| 12.2XH   | Short-lived early deployment release |            |  | 12.2(1)XH<br>2001-June-25 |
| 12.2XQ   | Short-lived early deployment release |            |  | 12.2(1)XQ<br>2001-June-23 |
| Notes  |                                      |            |  |                           |
| <p>* All dates are estimates and subject to change.</p> <p>** Interim releases are subjected to less rigorous testing than regular maintenance releases, and may have serious bugs.</p> <p>IOS releases 12.2(1a) and 12.2(1b) are deferred for the following platforms: ICS, 1750,2600,3600, vg200,5300,5800, 7200, 7500, 3810</p> |                                      |            |  |                           |

## Workarounds

The workaround for this vulnerability is to disable HTTP server on the router or to use TACACS+ or Radius for authentication.

To disable HTTP server, use the following commands:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# no ip http server
```

**Note:** This workaround is not applicable to customers running 12.2(2)T releases with IPv6 enabled because of CSCdt93862. In the 12.2(2)T release, HTTP is still accessible via IPv6 regardless of whether the HTTP server is disabled in the configuration. Customers running the 12.2(2)T release with IPv6 enabled must upgrade to 12.2(2.2)T or higher release (12.2(2)T1 being the preferred release). IPv6 support is not enabled by default.

To configure TACACS+ or Radius for authentication, please consult the following link <http://www.cisco.com/warp/public/480/tacplus.shtml>.

## 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](mailto: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 has been reported to us independently by David Hyams, Ernst & Young, Switzerland and by Bashis ([bash@ns.wcd.se](mailto:bash@ns.wcd.se)).

The Cisco PSIRT have learned that an automated exploit has been created. The scanning for and attempts of exploiting this vulnerability are increasing. All customers are strongly recommended to apply workarounds or to upgrade to the IOS version that is not affected.

## 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 notice will be posted on Cisco's Worldwide Web site at <http://www.cisco.com/warp/public/707/cisco-sa-20010627-ios-http-level.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](mailto:cust-security-announce@cisco.com)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [comp.dcom.sys.cisco](mailto:comp.dcom.sys.cisco)
- [firewalls@lists.gnac.com](mailto:firewalls@lists.gnac.com)
- Various internal Cisco mailing lists

Future updates of this advisory, 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 above URL for any updates.

## Revision History

|              |              |   |
|--------------|--------------|---|
| Revision 1.8 | 2003-Sep-23  | Updated 2nd paragraph in Exploitation and Public Announcements section                          |
| Revision 1.7 | 2001-Sep-13  | Updated status from interim to final.   |
| Revision 1.6 | 2001-Sep-10  | Updated workarounds section.  |
| Revision 1.5 | 2001-Aug-08  | Updated Affected Products to include Catalyst 3500 XL   |
| Revision 1.4 | 2001-July-19 | Revised Affected Products, IOS table, and Workarounds sections.                                 |
| Revision 1.3 | 2001-July-13 | Updated workarounds section; deleted Catalyst 1900 and 2800 from the Affected Products section. |
| Revision     | 2001-June-29 | Updated platform descriptions   |

|                 |                         |  |
|-----------------|-------------------------|--|
| 1.2             |                         |  |
| Revision<br>1.1 | <del>2001–June–28</del> | <del>Updated software availability dates</del> |
| Revision<br>1.0 | <del>2001–June–27</del> | <del>Initial public release</del>              |

## 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](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: Sep 23, 2003

Document ID: 13626

---