

Cisco Security Advisory: Cisco IOS Software Authentication Proxy Vulnerability

Advisory ID: cisco-sa-20090923-auth-proxy

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-auth-proxy.shtml>

Revision 1.1

Last Updated 2009 October 19 1600 UTC (GMT)

For Public Release 2009 September 23 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

[Summary](#)

[Affected Products](#)

[Details](#)

[Vulnerability Scoring 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

Cisco IOS® Software configured with Authentication Proxy for HTTP(S), Web Authentication or the consent feature, contains a vulnerability that may allow an unauthenticated session to bypass the authentication proxy server or bypass the consent webpage.

Cisco has released free software updates that address this vulnerability.

There are no workarounds that mitigate this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20090923-auth-proxy.shtml>

Note: The September 23, 2009, Cisco IOS Security Advisory bundled publication includes eleven Security Advisories. Ten of the advisories address vulnerabilities in Cisco IOS Software, and one advisory addresses a vulnerability in Cisco Unified Communications Manager. Each advisory lists the releases that correct the vulnerability or vulnerabilities detailed in the advisory.

Individual publication links are in "Cisco Event Response: Semiannual Cisco IOS Software Advisory Bundled Publication" at the following link:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep09.html

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ Affected Products

☐ Vulnerable Products

Devices running affected versions of Cisco IOS Software and configured with Authentication Proxy for HTTP(S) or Web Authentication or the consent feature are vulnerable.

To determine the Cisco IOS Software release that is running on a Cisco product, administrators can log in to the device and issue the **show version** command to display the system banner. The system banner confirms that the device is running Cisco IOS Software by displaying text similar to "Cisco Internetwork Operating System Software" or "Cisco IOS Software." The image name displays in parentheses, followed by "Version" and the Cisco IOS Software release name. Other Cisco devices do not have the **show version** command or may provide different output.

The following example identifies a Cisco product that is running Cisco IOS Software Release 12.3(26) with an installed image name of C2500-IS-L:

```
Router#show version
Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-IS-L), Version 12.3(26),
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
```

Copyright ©) 1986-2008 by cisco Systems, Inc.
Compiled Mon 17-Mar-08 14:39 by dchih

<output truncated>

The following example shows a product that is running Cisco IOS Software release 12.4(20)T with an image name of C1841-ADVENTERPRISEK9-M:

```
Router#show version
Cisco IOS Software, 1841 Software (C1841-ADVENTERPRISEK9-M),
Version 12.4(20)T, RELEASE SOFTWARE (fc3)
Technical Support: http://www.cisco.com/techsupport
Copyright ©) 1986-2008 by Cisco Systems, Inc.
Compiled Thu 10-Jul-08 20:25 by prod_rel_team
```

<output truncated>

Additional information about Cisco IOS Software release naming conventions is available in "White Paper: Cisco IOS Reference Guide" at the following link: <http://www.cisco.com/warp/public/620/1.html>.

To determine if your device is configured with either Authentication Proxy for HTTP(S), Web Authentication or the consent feature, log into the device and issue the **show running-config** command.

The following example identifies firewall authentication proxy services using the ip auth-proxy under the proxy rule name example_auth_proxy_name:

```
Router#show running-config
<output truncated>

!
! Set up the aaa new model to use the authentication proxy.
!

aaa authorization auth-proxy default group

!
! Apply a name to the authentication proxy configuration
rule.
!

ip auth-proxy name example_auth_proxy_name http

!
! Apply the authentication proxy rule at an interface.
!

interface e0
```

```
ip auth-proxy example_auth_proxy_name
```

```
!
```

```
<output truncated>
```

The following example identifies firewall authentication proxy services running for HTTP under the proxy rule name `example_auth_proxy_name`, using the `ip admission` commands. This is the same configuration as Web Authentication:

```
Router#show running-config
```

```
<output truncated>
```

```
!
```

```
! Set up the aaa new model to use the authentication proxy.
```

```
!
```

```
aaa authorization auth-proxy default group
```

```
!
```

```
! Apply a name to the authentication proxy configuration rule.
```

```
!
```

```
ip admission name example_auth_proxy_name proxy http  
inactivity-time 60
```

```
!
```

```
! Apply the authentication proxy rule at an interface.
```

```
!
```

```
interface FastEthernet0/1  
ip admission example_auth_proxy_name
```

```
!
```

```
<output truncated>
```

The following example identifies a device configured with the consent feature under the consent rule name `example_consent_rule`:

```
Router#show running-config
```

```
<output truncated>
```

```
!
```

```
! Apply a name to the consent configuration rule.
```

```
!
```

```
ip admission name example_consent_rule consent

!  
! Apply the consent rule at an interface.  
!  
  
interface FastEthernet 0/0  
  ip admission consent-rule_rule  
  
!  
  
<output truncated>
```

☐ Products Confirmed Not Vulnerable

The following products and features are not affected by this vulnerability:

- Cisco IOS XR Software
- Cisco IOS XE Software
- Firewall Authentication Proxy for FTP and Telnet Sessions
- Cisco IOS devices not configured with Authentication Proxy for HTTP(S) or the consent feature

No other Cisco products are currently known to be affected by this vulnerability.

[Top of the section](#) [Close Section](#)

☐ Details

The Cisco IOS Firewall authentication proxy feature allows network administrators to apply specific security policies on a per-user basis. With the authentication proxy feature, users can log in to the network or access the Internet via HTTP, and their specific access profiles are automatically retrieved and applied from a CiscoSecure ACS, or other RADIUS or TACACS+ authentication server. The user profiles are active only when there is active traffic from the authenticated users. Web Authentication feature leverages the underlying authentication proxy feature.

The consent feature for Cisco IOS routers enables organizations to provide temporary Internet and corporate access to end users through their wired and wireless networks by presenting a consent webpage. The consent feature can be used with or without requesting a username and password, but still leverages the underlying authentication proxy feature.

This vulnerability allows a session to be permitted without first being authenticated by the authentication proxy, or to be permitted without first acknowledging the consent webpage. At least one successfully authenticated session or accepted consent session must exist for the vulnerability to be exposed. When this occurs, the RADIUS or TACACS+ server will show subsequent users as authenticated, all with the same username as the initial connection if performing authentication, regardless of the authentication information

provided by the user and whether it was defined on the AAA server, and regardless of whether the password was correct.

This vulnerability is caused by a race condition in the code, and several conditions outside the control of a malicious user and must be met before this vulnerability could be exploited.

For further information on Authentication Proxy for HTTP see the Cisco IOS Security Configuration Guide, Release 12.4 "Configuring Authentication Proxy" at the following link: http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_cfg_authen_prxy_external_docbase_0900e4b1805afd05_4container_external_docbase_0900e4b1807b01d5.html

For further information on Authentication Proxy for HTTPS see the Cisco IOS Security Configuration Guide, Release 12.4 "Firewall Support of HTTPS Authentication Proxy" at the following link: http://www.cisco.com/en/US/docs/ios/security/configuration/guide/sec_fwall_https_prxy_external_docbase_0900e4b1805afe18_4container_external_docbase_0900e4b1807b01d5.html

For further information on the consent feature see the Cisco IOS Security Configuration Guide, Securing User Services, Release 12.2SR "Consent Feature for Cisco IOS Routers" at the following link: http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cons_feat_rtrs_ps6922_TSD_Products_Configuration_Guide_Chapter.html

For further information on the Web Authentication feature see the Catalyst 3750 Switch Software Configuration Guide, Release 12.2(50)SE "Configuring IEEE 802.1x Port-Based Authentication" at the following link: http://www.cisco.com/en/US/docs/switches/lan/catalyst3750/software/release/12.2_50_se/configuration/guide/sw8021x.html#wp1401291

This vulnerability is documented in the following Cisco Bug ID: [CSCsy15227](#) ([registered](#) customers only) and has been assigned the Common Vulnerabilities and Exposures (CVE) identifier CVE-2009-2863.

[Top of the section](#) [Close Section](#)

☐ Vulnerability Scoring Details

Cisco has provided scores for the vulnerability in this advisory based on the Common Vulnerability Scoring System (CVSS). The CVSS scoring in this Security Advisory is done in accordance with CVSS version 2.0.

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

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

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> .

CSCsy15227: Cisco IOS Software Authentication Proxy Vulnerability					
Calculate the environmental score of CSCsy15227					
CVSS Base Score - 7.1					
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact
Network	Medium	None	Complete	None	None
CVSS Temporal Score - 5.9					
Exploitability		Remediation Level		Report Confidence	
Functional		Official-Fix		Confirmed	

[Top of the section](#) [Close Section](#)

☐ Impact

Successful exploitation of the vulnerability may result in an unauthenticated and unauthorized user bypassing the authentication proxy services offered in Cisco IOS Authentication Proxy for HTTP(S) and/or bypassing the consent accept webpage.

[Top of the section](#) [Close Section](#)

☐ Software Versions 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) names a Cisco IOS release train. If a given release train is vulnerable, then the earliest possible releases that contain the fix (along with the anticipated date of availability for each, if applicable) are listed in the "First Fixed Release" column of the table. The "Recommended Release" column indicates the releases which have fixes for all the published vulnerability at the time of this Advisory. 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. Cisco recommends upgrading to a release equal to or later than the release in the "Recommended Releases" column of the table.

Major Release	Availability of Repaired Releases	
Affected 12.0-Based Releases	First Fixed Release	Recommended Release
12.0	Not Vulnerable	
12.0DA	Not Vulnerable	
12.0DB	Releases up to and including 12.0(4) DB are not vulnerable. Releases 12.0(7) DB and later are not vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0DC	Releases up to and including 12.0(3) DC1 are not vulnerable. Releases 12.0(7) DC and later are not vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0S	Not Vulnerable	
12.0SC	Not Vulnerable	

12.0SL	Not Vulnerable	
12.0SP	Not Vulnerable	
12.0ST	Not Vulnerable	
12.0SX	Not Vulnerable	
12.0SY	Not Vulnerable	
12.0SZ	Not Vulnerable	
12.0T	Vulnerable; first fixed in 12.4 Releases up to and including 12.0(4) T1 are not vulnerable.	12.4(23b) 12.4(25b)
12.0W	Not Vulnerable	
12.0WC	Releases prior to 12.0(5)WC4 are vulnerable, release 12.0(5)WC4 and later are not vulnerable	
12.0WT	Not Vulnerable	
12.0XA	Not Vulnerable	
12.0XB	Not Vulnerable	
12.0XC	Not Vulnerable	
12.0XD	Not Vulnerable	

12.0XE	Vulnerable; first fixed in 12.4 Releases up to and including 12.0(5) XE are not vulnerable.	12.4(23b) 12.4(25b)
12.0XF	Not Vulnerable	
12.0XG	Not Vulnerable	
12.0XH	Not Vulnerable	
12.0XI	Not Vulnerable	
12.0XJ	Not Vulnerable	
12.0XK	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.0XL	Not Vulnerable	
12.0XM	Not Vulnerable	
12.0XN	Not Vulnerable	
12.0XQ	Not Vulnerable	
12.0XR	Vulnerable; first fixed in 12.4 Releases up to and including 12.0(6) XR are not vulnerable.	12.4(23b) 12.4(25b)
12.0XS	Not Vulnerable	

12.0XT	Not Vulnerable	
12.0XV	Not Vulnerable	
Affected 12.1- Based Releases	First Fixed Release	Recommended Release
12.1	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1AA	Not Vulnerable	
12.1AX	Not Vulnerable	
12.1AY	Releases up to and including 12.1(13) AY are not vulnerable. Releases 12.1(22) AY1 and later are not vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.1AZ	Not Vulnerable	
12.1CX	Not Vulnerable	
12.1DA	Not Vulnerable	
12.1DB	Releases up to and including 12.1(3) DB1 are not vulnerable. Releases 12.1(4) DB1 and later are not vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)

12.1DC	<p>Releases up to and including 12.1(4) DC are not vulnerable.</p> <p>Releases 12.1(4) DC2 and later are not vulnerable; first fixed in 12.4</p>	<p>12.4(23b)</p> <p>12.4(25b)</p>
12.1E	<p>Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory</p>	
12.1EA	<p>Releases up to and including 12.1(6) EA1a are not vulnerable.</p> <p>Releases 12.1(8) EA1c and later are not vulnerable; first fixed in 12.2SE</p>	<p>12.2(50)SE3; Available on 13-OCT-2009</p>
12.1EB	<p>Not Vulnerable</p>	
12.1EC	<p>Not Vulnerable</p>	
12.1EO	<p>Not Vulnerable</p>	
12.1EU	<p>Not Vulnerable</p>	
12.1EV	<p>Not Vulnerable</p>	
12.1EW	<p>Not Vulnerable</p>	

12.1EX	Vulnerable; first fixed in 12.4 Releases up to and including 12.1(2) EX are not vulnerable.	12.4(23b) 12.4(25b)
12.1EY	Not Vulnerable	
12.1EZ	Not Vulnerable	
12.1GA	Not Vulnerable	
12.1GB	Not Vulnerable	
12.1T	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XA	Not Vulnerable	
12.1XB	Not Vulnerable	
12.1XC	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XD	Not Vulnerable	
12.1XE	Not Vulnerable	
12.1XF	Not Vulnerable	
12.1XG	Not Vulnerable	
12.1XH	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)

12.1XI	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XJ	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XL	Releases prior to 12.1(3a)XL2 are vulnerable, release 12.1(3a)XL2 and later are not vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XM	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XP	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XQ	Not Vulnerable	
12.1XR	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1XS	Not Vulnerable	
12.1XT	Vulnerable; first fixed in 12.4 Releases up to and including 12.1(2) XT2 are not vulnerable.	12.4(23b) 12.4(25b)
12.1XU	Not Vulnerable	
12.1XV	Not Vulnerable	
12.1XW	Not Vulnerable	

12.1XX	Not Vulnerable	
12.1XY	Not Vulnerable	
12.1XZ	Not Vulnerable	
12.1YA	Not Vulnerable	
12.1YB	Vulnerable; first fixed in 12.4 Releases up to and including 12.1(5) YB are not vulnerable.	12.4(23b) 12.4(25b)
12.1YC	Not Vulnerable	
12.1YD	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1YE	Releases prior to 12.1(5)YE6 are vulnerable, release 12.1(5)YE6 and later are not vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1YF	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.1YH	Not Vulnerable	
12.1YI	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	

12.1YJ	Not Vulnerable	
Affected 12.2- Based Releases	First Fixed Release	Recommended Release
12.2	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2B	Vulnerable; first fixed in 12.4 Releases up to and including 12.2(2) B7 are not vulnerable.	12.4(23b) 12.4(25b)
12.2BC	Not Vulnerable	
12.2BW	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2BX	Not Vulnerable	
12.2BY	Not Vulnerable	
12.2BZ	Not Vulnerable	
12.2CX	Not Vulnerable	
12.2CY	Not Vulnerable	
12.2CZ	Vulnerable; migrate to any release in 12.2SB	12.2(31)SB16 12.2(33)SB7
12.2DA	Not Vulnerable	

12.2DD	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2DX	Not Vulnerable	
12.2EW	Not Vulnerable	
12.2EWA	Not Vulnerable	
12.2EX	Vulnerable; first fixed in 12.2SE Releases up to and including 12.2(37) EX are not vulnerable.	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.2EY	Vulnerable; first fixed in 12.2SE Releases up to and including 12.2(25) EY4 are not vulnerable.	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.2EZ	Not Vulnerable	
12.2FX	Not Vulnerable	
12.2FY	Not Vulnerable	
12.2FZ	Vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.2IRA	Vulnerable; first fixed in 12.2SRD	12.2(33)SRD3
12.2IRB	Vulnerable; first fixed in 12.2SRD	12.2(33)SRD3

12.2IRC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2IXA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2IXB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2IXC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2IXD	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	

12.2IXE	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2IXF	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2IXG	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2IXH	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2JA	Not Vulnerable	
12.2JK	Not Vulnerable	
12.2MB	Not Vulnerable	
12.2MC	Not Vulnerable	

12.2S	Note: Releases prior to 12.2(30)S are vulnerable, release 12.2(30)S and later are not vulnerable;	12.2(31)SB16 12.2(33)SB7
12.2SB	Not Vulnerable	
12.2SBC	Note: Releases prior to 12.2(27)SBC3 are vulnerable, release 12.2(27)SBC3 and later are not vulnerable;	12.2(31)SB16 12.2(33)SB7
12.2SCA	Not Vulnerable	
12.2SCB	Not Vulnerable	
12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.2SEA	Not Vulnerable	
12.2SEB	Not Vulnerable	
12.2SEC	Vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.2SED	Vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.2SEE	Vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009

12.2SEF	Releases prior to 12.2(25)SEF2 are vulnerable, release 12.2(25)SEF2 and later are not vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.2SEG	Releases prior to 12.2(25)SEG4 are vulnerable, release 12.2(25)SEG4 and later are not vulnerable; first fixed in 12.2SE	12.2(50)SE3 12.2(52)SE; Available on 13-OCT-2009
12.2SG	12.2(50)SG4 12.2(53)SG1; Available on 07-DEC-2009	12.2(50)SG4
12.2SGA	12.2(31)SGA11; Available on 04-DEC-2009	12.2(31)SGA11; Available on 04-DEC-2009
12.2SL	Not Vulnerable	
12.2SM	Not Vulnerable	
12.2SO	Not Vulnerable	
12.2SQ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2SRA	Vulnerable; first fixed in 12.2SRD	12.2(33)SRD3
12.2SRB	Vulnerable; first fixed in 12.2SRD	12.2(33)SRD3

12.2SRC	12.2(33)SRC5; Available on 29- OCT-2009	12.2(33)SRD3
12.2SRD	12.2(33)SRD2a 12.2(33)SRD3	12.2(33)SRD3
12.2STE	Not Vulnerable	
12.2SU	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2SV	Not Vulnerable	
12.2SVA	Not Vulnerable	
12.2SVC	Not Vulnerable	
12.2SVD	Not Vulnerable	
12.2SVE	Not Vulnerable	
12.2SW	Not Vulnerable	
12.2SX	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2SXA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	

12.2SXB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2SXD	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2SXE	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2SXF	12.2(18)SXF17; Available on 30-SEP-2009 Please see IOS Software Modularity Patch	12.2(18)SXF17; Available on 30-SEP-2009
12.2SXH	12.2(33)SXH6; Available on 30-OCT-2009 Please see IOS Software Modularity Patch	12.2(33)SXH6; Available on 30-OCT-2009
12.2SXI	12.2(33)SXI2 12.2(33)SXI2a	12.2(33)SXI2a

12.2SY	Not Vulnerable	
12.2SZ	Not Vulnerable	
12.2T	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2TPC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2XA	Vulnerable; first fixed in 12.4 Releases up to and including 12.2(1) XA are not vulnerable.	12.4(23b) 12.4(25b)
12.2XB	Vulnerable; first fixed in 12.4 Releases up to and including 12.2(2) XB1 are not vulnerable.	12.4(23b) 12.4(25b)
12.2XC	Not Vulnerable	
12.2XD	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XE	Not Vulnerable	
12.2XF	Not Vulnerable	

12.2XG	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XH	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XI	Not Vulnerable	
12.2XJ	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XK	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XL	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XM	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XNA	Not Vulnerable	
12.2XNB	Not Vulnerable	
12.2XNC	Not Vulnerable	
12.2XND	Not Vulnerable	
12.2XO	Vulnerable; first fixed in 12.2SG	12.2(31)SGA11 12.2(50)SG4
12.2XQ	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XR	Not Vulnerable	
12.2XS	Not Vulnerable	

12.2XT	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XU	Not Vulnerable	
12.2XV	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2XW	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2YA	Releases prior to 12.2(4)YA8 are vulnerable, release 12.2(4)YA8 and later are not vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2YB	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YD	Not Vulnerable	

12.2YE	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YF	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YG	Not Vulnerable	
12.2YH	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YJ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YK	Not Vulnerable	

12.2YL	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YM	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2YN	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YO	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YP	Not Vulnerable	
12.2YQ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	

12.2YR	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YS	Not Vulnerable	
12.2YT	Not Vulnerable	
12.2YU	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YV	Releases prior to 12.2(11)YV1 are vulnerable, release 12.2(11)YV1 and later are not vulnerable	
12.2YW	Not Vulnerable	
12.2YX	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2YY	Not Vulnerable	

12.2YZ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2ZA	Not Vulnerable	
12.2ZB	Not Vulnerable	
12.2ZC	Not Vulnerable	
12.2ZD	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2ZE	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2ZF	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2ZG	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.2ZH	Releases prior to 12.2(13)ZH6 are vulnerable, release 12.2(13)ZH6 and later are not vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)

12.2ZJ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2ZL	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2ZP	Not Vulnerable	
12.2ZU	Vulnerable; first fixed in 12.2SXH	12.2(33)SXH6; Available on 30-OCT-2009
12.2ZX	Not Vulnerable	
12.2ZY	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.2ZYA	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	

Affected 12.3- Based Releases	First Fixed Release	Recommended Release
12.3	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3B	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3BC	Not Vulnerable	
12.3BW	Not Vulnerable	
12.3EU	Not Vulnerable	
12.3JA	Not Vulnerable	
12.3JEA	Not Vulnerable	
12.3JEB	Not Vulnerable	
12.3JEC	Not Vulnerable	
12.3JK	Releases up to and including 12.3(2) JK3 are not vulnerable. Releases 12.3(8) JK1 and later are not vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3JL	Not Vulnerable	
12.3JX	Not Vulnerable	

12.3T	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3TPC	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.3VA	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3XA	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XB	Not Vulnerable	
12.3XC	Releases prior to 12.3(2)XC4 are vulnerable, release 12.3(2)XC4 and later are not vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XD	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XE	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)

12.3XF	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.3XG	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XI	Not Vulnerable	
12.3XJ	Not Vulnerable	
12.3XK	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XL	Vulnerable; first fixed in 12.4T	12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3XQ	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XR	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XS	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3XU	Not Vulnerable	
12.3XW	Not Vulnerable	
12.3XX	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)

12.3XY	Not Vulnerable	
12.3XZ	Not Vulnerable	
12.3YA	Vulnerable; first fixed in 12.4	12.4(23b) 12.4(25b)
12.3YD	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YF	Not Vulnerable	
12.3YG	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YH	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YI	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009

12.3YJ	Not Vulnerable	
12.3YK	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YM	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YQ	Not Vulnerable	
12.3YS	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YT	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.3YU	Not Vulnerable	
12.3YX	Not Vulnerable	

12.3YZ	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	
12.3ZA	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
Affected 12.4-Based Releases	First Fixed Release	Recommended Release
12.4	12.4(23a) 12.4(25a)	12.4(23b) 12.4(25b)
12.4GC	Not Vulnerable	
12.4JA	Not Vulnerable	
12.4JDA	Not Vulnerable	
12.4JDC	Not Vulnerable	
12.4JDD	Not Vulnerable	
12.4JK	Not Vulnerable	
12.4JL	Not Vulnerable	
12.4JMA	Not Vulnerable	

12.4JMB	Not Vulnerable	
12.4JX	Not Vulnerable	
12.4MD	Not Vulnerable	
12.4MDA	Not Vulnerable	
12.4MR	Releases prior to 12.4(19)MR1 are vulnerable, release 12.4(19)MR1 and later are not vulnerable	
12.4SW	Not Vulnerable	
12.4T	12.4(24)T1 12.4(20)T3 12.4(22)T2 12.4(15)T9	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XA	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XB	Not Vulnerable	

12.4XC	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XD	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XE	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XF	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XG	Not Vulnerable	
12.4XJ	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009

12.4XK	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XL	Not Vulnerable	
12.4XM	Not Vulnerable	
12.4XN	Not Vulnerable	
12.4XP	Not Vulnerable	
12.4XQ	Not Vulnerable	
12.4XR	Not Vulnerable	
12.4XT	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XV	Vulnerable; Contact your support organization per the instructions in Obtaining Fixed Software section of this advisory	

12.4XW	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XY	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4XZ	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4YA	Vulnerable; first fixed in 12.4T	12.4(15)T10 12.4(20)T4 12.4(22)T3 12.4(24)T2; Available on 23-OCT-2009
12.4YB	12.4(22)YB4	12.4(22)YB4
12.4YD	Not Vulnerable	
12.4YE	Not Vulnerable	

Cisco IOS Software Modularity - Maintenance Packs

Customers who are using Cisco IOS Software Modularity can apply the respective maintenance packs. More

information on Cisco IOS Software Modularity can be found at the following link: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/prod_bulletin0900aecd80313e15.html

The Maintenance Packs listed below can be downloaded at <http://www.cisco.com/go/pn>

Cisco IOS Software Modularity Maintenance Pack for 12.2SXF

Cisco IOS Software Release	Solution Maintenance Pack (MP)
12.2(18)SXF14	MP001
12.2(18)SXF15	MP001
12.2(18)SXF16	MP001

Cisco IOS Software Modularity Maintenance Pack for 12.2SXH

Cisco IOS Software Release	Solution Maintenance Pack (MP)
12.2(33)SXH5	MP001

[Top of the section](#) [Close Section](#)

Workarounds

There are no workarounds for this vulnerability.

[Top of the section](#) [Close Section](#)

Obtaining Fixed Software

Cisco has released free software updates that address this vulnerability. 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/en/US/docs/general/warranty/English/EU1KEN_.html, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact 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 agreements 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 do not hold a Cisco service contract, and customers who purchase through third-party vendors but are unsuccessful in obtaining fixed software through their point of sale should acquire 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

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

Refer to http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html for additional TAC contact information, including localized telephone numbers, and instructions and e-mail addresses for use in various languages.

[Top of the section](#) [Close Section](#)

☐ Exploitation and Public Announcements

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

this advisory.

This vulnerability was discovered by Cisco during internal testing. The Cisco PSIRT is not aware of malicious exploitation of this vulnerability, although we are aware of some customers who have seen this vulnerability triggered within their infrastructures.

[Top of the section](#) [Close Section](#)

☐ **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.

[Top of the section](#) [Close Section](#)

☐ **Distribution**

This advisory is posted on Cisco's worldwide website at :

<http://www.cisco.com/warp/public/707/cisco-sa-20090923-auth-proxy.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-bulletins@lists.first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- 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.

[Top of the section](#) [Close Section](#)

☐ Revision History

Revision 1.1	2009-October-19	Updated ION software table.
Revision 1.0	2009-September-23	Initial public release

[Top of the section](#) [Close Section](#)

☐ 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>.

[Top of the section](#) [Close Section](#)

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)



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

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 - 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)