

Cisco Security Advisory: Access Point Web-browser Interface Vulnerability

Document ID: 70567

Advisory ID: cisco-sa-20060628-ap

<http://www.cisco.com/warp/public/707/cisco-sa-20060628-ap.shtml>

Revision 1.2

Last Updated 2006 September 20 1900 UTC (GMT)

For Public Release 2006 June 28 1700 UTC (GMT)

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

[Summary](#)

[Affected Products](#)

[Details](#)

[Impact](#)

[Software Version and Fixes](#)

[Workarounds](#)

[Obtaining Fixed Software](#)

[Exploitation and Public Announcements](#)

[Status of this Notice: FINAL](#)

[Distribution](#)

[Revision History](#)

[Cisco Security Procedures](#)

Summary

The Cisco web-browser interface for Cisco access points and Cisco 3200 Series Wireless Mobile Interface Card (WMIC), contains a vulnerability that could, under certain circumstances, remove the default security configuration from the managed access point and allow administrative access without validation of administrative user credentials.

Cisco has made free software available to address this vulnerability for affected customers. There are workarounds available to mitigate the effects of this vulnerability.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20060628-ap.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

The following access points are affected if running Cisco IOS® Software Releases 12.3(8)JA, 12.3(8)JA1 or 12.3(8)JK and are configured for web–interface management:

- 350 Wireless Access Point and Wireless Bridge
- 1100 Wireless Access Point
- 1130 Wireless Access Point
- 1200 Wireless Access Point
- 1240 Wireless Access Point
- 1310 Wireless Bridge
- 1410 Wireless Access Point
- Cisco 3200 Series Wireless Mobile Interface Card (WMIC)

To determine if web–interface management is enabled on a Cisco access point, log in to the device and issue the **show ip http server status** command. If the output shows either *http server status* or *http secure server status* as **enabled**, web–interface management is enabled. An example is shown below with web–interface management enabled:

```
ap#show ip http server status
    HTTP server status: Enabled
    HTTP server port: 80
[...lines removed...]
    HTTP secure server status: Disabled
    HTTP secure server port: 443
[...lines removed...]
```

Web–interface management (HTTP server) is enabled by default.

To check the version of Cisco IOS running on the access point:

- **Via Browser** Click on the **System Software** menu. The Cisco IOS software version will be displayed in the *System Software Version* field.
- **Via Command–Line Interface (CLI)** To determine the software running on a Cisco access point, log in to the device and issue the **show version** command to display the system banner.

Cisco IOS software will identify itself as "Internetwork Operating System Software" or simply "IOS".

On the next line of output, the image name will be displayed between parentheses, followed by "Version" and the Cisco IOS release name. Other Cisco devices will not have the **show version** command or will give different output.

The following example identifies a Cisco access point running Cisco IOS Software Release 12.3(7)JA1 with an installed image name of C1200–K9W7–M:

```
ap#show version
Cisco IOS Software, C1200 Software (C1200-K9W7-M),
Version 12.3(7)JA1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986–2005 by Cisco Systems, Inc.
Compiled Thu 06-Oct-05 09:40 by evmiller
!
[...lines removed...]
!
```

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

Products Confirmed Not Vulnerable

These products are not vulnerable:

- Access points that are not running Cisco IOS software
- Access points that are running any version of Cisco IOS other than Cisco IOS Software Releases 12.3(8)JA, 12.3(8)JA1, or 12.3(8)JK
- Access points with disabled web–interface management (both HTTP and HTTP secure)
- All Cisco access points running in lightweight mode

Details

The web–browser interface contains management pages that are used to change the wireless device settings, upgrade firmware, and monitor and configure other wireless devices on the network. The web–browser interface is enabled by default, and is indicated by the configuration command **ip http server** or **ip http secure–server**.

An access point running a default configuration will use the default enable secret password for administrative access. This can be modified via the web–browser interface tab **Security > Admin Access > Default Authentication (Global Password)** or via the CLI with the configuration command **enable secret [new_secret]**.

Local User List Only (Individual Passwords) allows administrators of the access points to define a local unique username/password database for their administrators, so that a common global password is not shared.

A vulnerability exists in the access point web–browser interface when **Security > Admin Access** is changed from **Default Authentication (Global Password)** to **Local User List Only (Individual Passwords)**. This results in the access point being re–configured with no security, either Global Password or Individual Passwords, enabled. This allows for open access to the access point via the web–browser interface or via the console port with no validation of user credentials.

Access points configured for **Local User List Only (Individual Passwords)** and running non–vulnerable versions of Cisco IOS which are subsequently upgraded to a vulnerable version of IOS are not affected by this vulnerability as long as the configuration is not altered after the upgrade.

This vulnerability is documented by Cisco bug ID [CSCsd67403](#) ([registered](#) customers only) Cannot Select Option to Authenticate using Local User List Only.

Impact

Successful exploitation of this vulnerability will result in unauthorized administrative access to the access point via the web–management interface or via the console port.

Software Version and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center (TAC) or your contracted maintenance provider for assistance.

Each row of the Cisco IOS software table (below) describes a release train and the platforms or products for which it is intended. If a given release train is vulnerable, then the earliest possible releases that contain the fix (the First Fixed Release) and the anticipated date of availability for each are listed in the Rebuild and Maintenance columns. A device running a release in the given train that is earlier than the release in a specific column (less than the First Fixed Release) is known to be vulnerable. The release should be upgraded at least to the indicated release or a later version (greater than or equal to the First Fixed Release label).

For more information on the terms "Rebuild" and "Maintenance," consult the following URL:
<http://www.cisco.com/warp/public/620/1.html>.

Major Release	Availability of Repaired Releases	
	Rebuild	Maintenance
12.3		
12.3(8)JA	12.3(8)JA2	12.3(11)JA
12.3(8)JA1	12.3(8)JA2	12.3(11)JA
12.3(8)JK	Vulnerable – please contact TAC.	

Workarounds

Either of the following workarounds and mitigations may be used to help mitigate the effects of this vulnerability:

- **Disable Web-Based Management**

To prevent the use of the web-browser interface via:

- **Web-Based Management** Select the **Disable Web-Based Management** check box on the **Services > HTTP-Web Server** page and click **Apply**.
- **CLI** Log in to the device and issue these configuration commands (save the configuration upon exiting):

```
ap(config)#no ip http server
ap(config)#no ip http secure-server
ap(config)#exit
```

- **Configure via CLI**

Enabling **Local User List Only (Individual Passwords)** via the CLI rather than the web-browser interface will provide the access point with the desired protected configuration. Log in to the device and issue these configuration commands (save the configuration upon exiting):

```
ap#configure terminal

!--- Setup the username password pair first.

ap(config)#username test privilege 15 password test

!--- Enable AAA.

ap(config)#aaa new-model

!--- Enable aaa authentication to the local database.

ap(config)#aaa authentication login default local

!--- Enable aaa authorization to the local database.

ap(config)#aaa authorization exec default local

!--- Enable http authentication to AAA.
```

```
ap(config)#ip http authentication aaa
ap(config)#exit
```

- **Configure RADIUS/TACACS Server first**

Via the web-browser interface enabling any RADIUS/TACACS+ server within **Security > Server Manager > Corporate Servers** and then performing the option of **Security > Admin Access as Local User List Only (Individual Passwords)** will provide a workaround to this vulnerability.

Obtaining Fixed Software

Cisco will make free software to address this vulnerability for affected customers. This advisory will be updated as fixed software becomes available. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html>, or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

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

Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

Customers using Third Party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

Have your product serial number available and give the URL of this notice as evidence of your entitlement to

a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

Exploitation and Public Announcements

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

Status of this Notice: FINAL

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

Distribution

This advisory is posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20060628-ap.shtml>.

Revision History

Revision 1.2	2006-Sep-20	Updated Vulnerable Products section to include Cisco 3200 Series Wireless Mobile Interface Card (WMIC), and updated Software Versions and Fixes section to include 12.3(8)JK.
Revision 1.1	2006-July-06	Cisco IOS Software Release 12.3(11)JA release date changed in the Software Version and Fixes section.
Revision 1.0	2006-June-28	Initial public release.

Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.
