

# Cisco Security Advisory: HTTP GET Vulnerability in AP1x00

Document ID: 44162

Advisory ID: cisco-sa-20030728-ap1x00

<http://www.cisco.com/warp/public/707/cisco-sa-20030728-ap1x00.shtml>

## Revision 1.1

Last Updated 2003 July 28 1830 UTC (GMT)

For Public Release 2003 July 28 1600 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

A vulnerability has been reported by an external researcher in Cisco IOS<sup>®</sup> release for Cisco Aironet AP1x00 Series Wireless devices. The vulnerability affects only IOS-based Cisco Aironet Wireless products. The VxWorks based Cisco Aironet Wireless Devices are not affected. This vulnerability can cause the AP1x00 to reload and is documented as Cisco bug ID CSCeb49869 ( registered customers only) (also CAN-2003-0511). 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-20030728-ap1x00.shtml>.

The external report can be found at <http://www.vigilante.com/inetsecurity/advisories/VIGILANTE-2003001.htm> . A second external report found at <http://www.vigilante.com/inetsecurity/advisories/VIGILANTE-2003002.htm> details another issue, Cisco bug ID CSCdz29724 ( registered customers only) , which is present in all IOS software and is duplicated by the AP1x00 specific Cisco bug ID CSCeb49842 ( registered customers only) (also CAN-2003-512). More details on it can be found at <http://www.cisco.com/warp/public/707/cisco-sn-20030724-ios-enum.shtml>.

## Affected Products

This section provides details on affected products.

## Vulnerable Products

Only the following Cisco IOS–based wireless Access Points are affected:

Hardware Model	Software Release(s)
Cisco Aironet Wireless Access Point AP1100 series	12.2(4)JA, 12.2(4)JA1,
Cisco Aironet Wireless Access Point AP1200 series	12.2(8)JA, 12.2(11)JA
Cisco Aironet Wireless Bridge AP1400 series	12.2(8)JA, 12.2(11)JA
	12.2(11)JA

All previous VxWorks–based software releases for Cisco Aironet Access Point 1200 are not affected. That includes the following, and earlier, software releases: 11.56, 12.01T1, 12.02T1, 12.03T.

In order to determine your software release you should log on the Access Point using any account available and execute the following command:

```
access-point> show ver

Cisco Internetwork Operating System Software
IOS (tm) C1100 Software (C1100-K9W7-M), Version 12.2(8)JA, EARLY
DEPLOYMENT RELEASE SOFTWARE (fc1)          ^^^^^^^^^^
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by cisco Systems, Inc.
```

The Cisco IOS software version is displayed in the second line of the output. In this example it is 12.2(8)JA.

## Products Confirmed Not Vulnerable

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

## Details

Sending a malformed URL to the Cisco Aironet AP1x00 can cause the device to reload.

## Impact

Repeated exploitation of this vulnerability can lead to a prolonged Denial–of–Service (DoS) of the AP1x00.

## Software Versions and Fixes

The vulnerability is fixed in the 12.2(11)JA1 version of the software for all Cisco Aironet AP1x00 devices.

## Workarounds

There are two workarounds for this vulnerability. One is to use **access-class** or **access-list** commands to limit the access to legitimate hosts only, and another workaround is to disable HTTP and use SSH to administer the Cisco Aironet Access Point.

The example of using **access-class** is given here:

```
ap(config)# ip http access-class 10
ap(config)# access-list 10 permit host 10.0.0.1
```

In this example, host 10.0.0.1 is the only one that is allowed to access the AP. All other hosts are prohibited.

To disable HTTP and enable SSH use this example:

```
ap(config)# no ip http server
ap(config)# ip domain name <your-domain>
ap(config)# crypto key generate rsa
The name for the keys will be: ap.your-domain
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys ...[OK]
ap(config)# line vty 0 4
ap(config-line)# transport input ssh
```

Now you can connect to the Cisco Aironet AP using SSH client from your computer. There are many free and commercial versions of SSH software available.

In addition to the workarounds it is possible to mitigate the exposure by configuring ACLs on the device so that only legitimate hosts can use the http service. This can be done in the following way:

```
access-list 111 permit tcp host 10.0.0.1 host 10.0.0.50 eq www
```

In this example the host 10.0.0.1 is the only one that is allowed to access the device at 10.0.0.50. You will have to change host IP addresses and the ACL number to suit your configuration. This ACL will have to be applied to all interfaces and block all IP addresses assigned to the affected device.

## 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 is reported by Reda Zitouni from Vigilante. Their report can be found at <http://www.vigilante.com/inetsecurity/advisories/VIGILANTE-2003001.htm>.

The Cisco PSIRT is not aware of 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.

Cisco Security Advisory: HTTP GET Vulnerability in AP1x00

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 website at .

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)
- [full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [cisco@spot.colorado.edu](mailto:cisco@spot.colorado.edu)
- [cisco-nsp@puck.nether.net](mailto:cisco-nsp@puck.nether.net)
- [comp.dcom.sys.cisco](mailto:comp.dcom.sys.cisco)
- Various internal Cisco mailing lists

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

## Revision History

Revision 1.0	2003-July-28 16:00 UTC (GMT)	Initial public release.
Revision 1.1	2003-July-28 18:30 UTC (GMT)	Corrected external report URLs.

## 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](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>.

---

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

---

Updated: Jul 26, 2007

Document ID: 44162

---