

# Cisco Security Advisory: Aironet Telnet Vulnerability

Document ID: 22425

Advisory ID: cisco-sa-20020409-aironet-telnet

<http://www.cisco.com/warp/public/707/cisco-sa-20020409-aironet-telnet.shtml>

## Revision 1.0

For Public Release 2002 April 09 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

It is possible to cause a denial-of-service attack if Cisco Aironet products have Telnet access enabled. Telnet access is the only requirement for such an attack; there are no additional conditions.

The workaround for this vulnerability is to disable Telnet access.

No other Cisco product is vulnerable.

This advisory is available at  
<http://www.cisco.com/warp/public/707/cisco-sa-20020409-aironet-telnet.shtml>.

## Affected Products

This section provides details on affected products.

## Vulnerable Products

All releases up to, but excluding, 11.21 are vulnerable. The following hardware products are affected.

- Cisco Aironet Access Point 340 and 350
- Cisco Aironet Bridge 350

## Products Confirmed Not Vulnerable

Products not affected are:

- Cisco Aironet Bridge 340
- Cisco Aironet 4800 Series
- Cisco Aironet 4500 Series and 3500 Series
- Cisco Aironet 3100 Series

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

## Details

This vulnerability is documented as Cisco Bug ID **CSCdw81244**.

It is possible to cause Cisco Aironet products to reboot if Telnet access is enabled and a password is required for authorization. This can be accomplished by providing an invalid username and password. This vulnerability cannot be triggered via the web interface.

## Impact

By repeatedly exploiting this vulnerability an attacker can cause denial of service.

## Software Versions and Fixes

This vulnerability is fixed in release 11.21, which is available now.

## Workarounds

The workaround is to disable Telnet access. You can accomplish this by following the link, via the web interface, path to reach the Console/Telnet Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Console/Telnet** in the Services section of the page.
3. On that page, click on the radio button for **Disable Telnet**.

**Note:** You must use the web interface or be connected on the console since you will be unable to save your changes if you are using Telnet. After disabling Telnet, your Telnet session will be terminated.

## 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 issue was reported to Cisco by a customer. Cisco PSIRT is not aware of any malicious exploitation or

public discussion of this vulnerability.

## 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 website at <http://www.cisco.com/warp/public/707/cisco-sa-20020409-aironet-telnet.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 notice, if any, will be placed on Cisco's worldwide web server, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are encouraged to check the URL given above for any updates.

## Revision History

Revision 1.0	<del>2002-April-09</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 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: Apr 09, 2002

Document ID: 22425

---