

Cisco Security Advisory: Access to the Cisco Aironet 340 Series Wireless Bridge via Web Interface

Document ID: 13612

Advisory ID: cisco-sa-20010307-aironet340

<http://www.cisco.com/warp/public/707/cisco-sa-20010307-aironet340.shtml>

Revision 1.0

For Public Release 2001 March 07 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 view and modify the bridge's configuration via Web interface even when Web access is disabled in the configuration. This defect is documented as Cisco bug ID CSCdt52783. This defect is present in the following hardware models:

- Aironet AP4500,
- Aironet AP4800,
- Aironet BR100,
- Aironet BR500,
- Cisco Aironet AIR-BR340

The firmware release 8.55 is the first image which contains the fix. All previous firmware releases for listed devices are vulnerable. No other Aironet/Cisco Aironet wireless product is affected by this vulnerability. This advisory is available at the <http://www.cisco.com/warp/public/707/cisco-sa-20010307-aironet340.shtml>.

Affected Products

This section provides details on affected products.

Vulnerable Products

The following hardware models are affected:

- Aironet AP4500,
- Aironet AP4800,
- Aironet BR100,
- Aironet BR500,
- Cisco Aironet AIR-BR340

They are vulnerable to this defect if they are running any of the following firmware releases:

- 7.X
- 8.07
- 8.24

The release 8.55 is the first release where this vulnerability is fixed. No other Aironet/Cisco Aironet wireless products are affected by this defect.

Products Confirmed Not Vulnerable

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

Details

It is possible to view and modify the bridge's configuration, using Web interface, despite it being explicitly disabled. This vulnerability is exploitable over the wired and wireless link alike.

Impact

An attacker is able to modify the bridge's configuration. It is necessary for an attacker to obtain connectivity to the bridge. That can be done either using wired or wireless Ethernet interface.

Software Versions and Fixes

This defect is fixed in the release 8.55 of the software.

Workarounds

There is no workaround if an attack is coming from wired Ethernet interface.

To mitigate this vulnerability if an attack is coming over the wireless link the following actions may be taken:

- Change SSID to non guessable value.
- Turn on WEP encryption if possible.

- On bridges (BR100, BR500 and AIR-BR340) turn off access point mode. That will disallow direct access to the bridge by any client.

For the instruction on how to perform these operations on the Cisco Aironet 340 Series Wireless Bridge, please see: <http://www.cisco.com/univercd/cc/td/doc/product/wireless/aironet/bridge/brdgqs.htm>.

For more detailed description please consult "Using the Cisco Aironet 340 Series Wireless Bridges", which can be found at: <http://www.cisco.com/univercd/cc/td/doc/product/wireless/aironet/bridge/ebridge.pdf>. Information on SSID and other basic settings is on page 4–3. Information on bridge mode vs AP mode is on page 4–17.

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

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 vulnerabilities described in this advisory. This vulnerability was discovered by a customer.

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-20010307-aironet340.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
- bugtraq@securityfocus.com
- first-teams@first.org (includes CERT/CC)
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- 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	2001-March-07	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 Web site at 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: Mar 07, 2001

Document ID: 13612
