

# Cisco Security Advisory: SNMP Trap Reveals WEP Key in Cisco Aironet Access Point

Document ID: 46468

Advisory ID: cisco-sa-20031202-SNMP-trap

<http://www.cisco.com/warp/public/707/cisco-sa-20031202-SNMP-trap.shtml>

## Revision 1.0

For Public Release 2003 December 02 1700 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

Cisco Aironet Access Points (AP) running Cisco IOS® software will send any static Wired Equivalent Privacy (WEP) key in the cleartext to the Simple Network Management Protocol (SNMP) server if the **snmp-server enable traps wlan-wep** command is enabled. Affected hardware models are the Cisco Aironet 1100, 1200, and 1400 series. This command is disabled by default. The workaround is to disable this command. Any dynamically set WEP key will not be disclosed.

Cisco Aironet AP models running VxWorks operating system are not affected by this vulnerability. No other Cisco product is affected.

This advisory will be available at

<http://www.cisco.com/warp/public/707/cisco-sa-20031202-SNMP-trap.shtml>.

## Affected Products

This section provides details on affected products.

## Vulnerable Products

Cisco Aironet AP 1100, 1200, and 1400 series running Cisco IOS software are affected. The Cisco AP 350 running Cisco IOS software is not affected. APs running VxWorks-based operating system are not affected.

To determine if you are running Cisco IOS software, type the following command on your workstation, replacing "10.0.0.1" with the IP address of your AP.

```
host%telnet 10.0.0.1
```

If you are not presented with a menu in a graphic form but simply with a prompt (such as ap1200%), then you may be vulnerable.

To further confirm that you are running Cisco IOS software, type the **show version** command at the prompt. If the result of the command is similar to the example below, then you are running Cisco IOS software.

```
ap1200>show version
Cisco Internetwork Operating System Software
IOS (tm) C1200 Software (C1200-K9W7-M), Version 12.2(11)JA1, EARLY DEPLOYMENT RELEASE SOFTWARE (FC)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2003 by Cisco Systems, Inc.
Compiled Mon 07-Jul-03 13:48 by ccai
Image text-base: 0x00003000, data-base: 0x004D46F4
```

If you have determined that Cisco IOS software is being used on the AP, execute the following command.

```
ap1200#show running
.
.
.
.
snmp-server enable traps tty
snmp-server enable traps dot11-qos
snmp-server enable traps wlan-wep <<<<<<
....
```

If your configuration contains the line marked with << , then you are vulnerable.

## Products Confirmed Not Vulnerable

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

## Details

If enabled, the **snmp-server enable traps wlan-wep** command will send static WEP keys in the cleartext to the SNMP server every time a key is changed or the AP is rebooted. This vulnerability is opportunistic, and the following conditions must be met for the vulnerability to be exploited.

- The **snmp-server enable traps wlan-wep** command must be enabled. (It is disabled by default.)
- An adversary must be able to intercept SNMP packets sent from the AP to the SNMP server.
- The AP in question must be rebooted or the static WEP key must be changed.

Under these circumstances, an adversary will be able to intercept all static WEP keys.

Dynamically configured WEP keys are not affected by this vulnerability and will not be revealed. A WEP key is dynamically configured if you are using one of the Extensible Authentication Protocol (EAP) authentication

protocols. The following EAP authentication protocols are currently supported in Cisco APs: LEAP, EAP-TLS, PEAP, EAP-MD5, and EAP-SIM.

This vulnerability is assigned Cisco [Bug ID CSCec55538](#) ([registered](#) customers only) .

## Impact

By being able to intercept a static WEP key, an attacker can drastically reduce the effort to break WEP encryption. Please note that this is true only for cases in which you are not using one of the EAP authentication types but are using only static WEP keys.

## Software Versions and Fixes

The vulnerable Cisco IOS software releases are 12.2(8)JA, 12.2(11)JA and 12.2(11)JA1.

The first fixed release is 12.2(13)JA1.

## Workarounds

The workaround is to disable the associated SNMP trap command by typing the following global command.

```
ap1200(config)#no snmp-server enable traps wlan-wep
```

While the above command will stop the AP from sending your WEP key, Cisco recommends that you do not use static WEP keys but use some of the EAP authentication protocols supported by the AP. The WEP scheme itself has several severe drawbacks. For more details regarding wireless LAN security, please see [http://www.cisco.com/application/pdf/en/us/guest/netsol/ns386/c649/ccmigration\\_09186a0080871da5.pdf](http://www.cisco.com/application/pdf/en/us/guest/netsol/ns386/c649/ccmigration_09186a0080871da5.pdf). The papers there are regarding general wireless security and provide configuration examples.

## 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

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 Bill Van Devender.

## 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 will be posted on Cisco's worldwide website at <http://www.cisco.com/warp/public/707/cisco-sa-20031202-SNMP-trap.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)
- [first-teams@first.org](mailto:first-teams@first.org) (includes CERT/CC)
- [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com)
- [full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)
- [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)
- [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 Dec 02	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](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>.

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#) © 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Dec 02, 2003

Document ID: 46468

---