

[NEWS] SNMP Trap Reveals WEP Key in Cisco Aironet Access Point

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0010.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/03/03

To: list@securiteam.com

Date: 3 Dec 2003 15:47:23 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

SNMP Trap Reveals WEP Key in Cisco Aironet Access Point

SUMMARY

Cisco Aironet Access Points (AP) running Cisco IOS® software will send any static Wired Equivalent Privacy (WEP) key in the clear text 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.

DETAILS

Affected 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

Securiteam: [NEWS] SNMP Trap Reveals WEP Key in Cisco Aironet Access Point

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 (fc1)
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

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind. In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.