

Cisco Aironet AP1100 Valid Account Disclosure Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-07/0356.html>

From: zitouni (reda.zitouni_at_vigilante.com)

Date: 07/28/03

Date: 28 Jul 2003 16:49:23 -0000

To: bugtraq@securityfocus.com

('binary' encoding is not supported, stored as-is)

VIGILANTE Security Watch Advisory

Name: Cisco Aironet AP1100 Valid Account Disclosure Vulnerability
Systems Affected: Tested on a Cisco Aironet AP1100 Model 1120B Series
Wireless device.

Firmware version 12.2(4)JA and earlier.

NB : A large number of Cisco IOSes are affected by this flaw.

Severity: High Risk

Vendor URL: <http://www.vigilante.com>

Authors: Reda Zitouni (reda.zitouni@vigilante.com)

Date: 28th July 2003

Advisory Code: VIGILANTE-2003002

Description

Cisco Aironet 1100 Series Access Point is a device manufactured by Cisco Systems offering a WLAN solution based on the 802.11b Wifi standard. The Aironet Bridge is vulnerable to a Brute Force attack revealing if an account exists or not.

Details

A flaw in firmware version 12.2(4)JA and earlier allows a malicious remote user to discover which accounts are valid on the targeted Cisco Aironet Access Point by using classical brute force techniques. Exploitation of this flaw is possible if the telnet service is enabled with authentication.

If an attacker submits an existing account as login he will be then prompted for the password. If not the case a ""% Login invalid" reply will be displayed by the server, revealing the account is not existing. By default on the Aironet AP1100, the 'cisco' account is set and is prompted for a password when submitted. That default account then allows

SecurityFocus Bugtraq: Cisco Aironet AP1100 Valid Account Disclosure Vulnerability

an attacker to determine if this flaw on the remote device is patched or not. This may lead to further serious attacks.

Vendor status:

Cisco was contacted June 19, 2003 and answered the same day. 5 days later, they told us that they would release a patch soon. The patch was finally released July 3, 2003. Please note that this flaw is released by Cisco as a Security Notice in CCO.

Vulnerability Assessment:

A test case to detect this vulnerability was added to SecureScan NX in the upgrade package of July 28, 2003. You can see the documentation of this test case 15438 on SecureScan NX web site at

<http://securescannx.vigilante.com/tc/15438>.

Fix: A firmware upgrading the Aironet IOS version to c1100-k9w7 has been released by Cisco. Please note that this version fixes some other bugs as TC 17655 (refer to release note).

Workaround:

Restrict access to your telnet service from outside your WLAN. A stronger authentication mechanism, such as SSH can also be implemented.

CVE: Common Vulnerabilities and Exposures group (reachable at <http://cve.mitre.org/>) was contacted and assigned CAN-2003-0512 to this vulnerability.

Links:

Cisco Advisory: <http://www.cisco.com/warp/public/707/cisco-sn-20030724-ios-enum.shtml>

Vigilante Advisory:

<http://www.vigilante.com/inetsecurity/advisories/VIGILANTE-2003002.htm>

Product Homepage: <http://www.cisco.com/warp/public/cc/pd/witc/ps4570>

CVE: CAN-2003-0512 <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-CAN-2003-0512>

Credit:

This vulnerability was discovered by Reda Zitouni, member of our Security Watch Team at VIGILANTE.

We wish to thank Cisco PSIRT Team for their fast answer to fix this problem.

Copyright VIGILANTE.com, Inc. 2003-07-28

Disclaimer:

The information within this document may change without notice. Use of

SecurityFocus Bugtraq: Cisco Aironet AP1100 Valid Account Disclosure Vulnerability

this information constitutes acceptance for use in an AS IS condition. There are NO warranties with regard to this information. In no event shall the author be liable for any consequences whatsoever arising out of or in connection with the use or spread of this information. Any use of this information lays within the user's responsibility.

Feedback:

Please send suggestions, updates, and comments to securitywatch@vigilante.com