

[NEWS] Apple AirPort Administrative Password Obfuscation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-05/0030.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/18/03

To: list@securiteam.com

Date: 18 May 2003 12:50:02 +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

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Apple AirPort Administrative Password Obfuscation

SUMMARY

Apple's AirPort device is a wireless access point, providing 802.11 services to network clients. Authentication credentials are obfuscated, and then sent over the network. If an AirPort is administered over the Ethernet interface or via an insecure (non-WEP) wireless connection, an attacker that can sniff the network can obtain administrative access to the AirPort.

DETAILS

Vulnerable systems:

* AirPort Base Station (ALL)

Apple's AirPort device is a wireless access point, providing 802.11 services to network clients. This device is managed through a proprietary administrative protocol over a TCP port (5009/tcp). Authentication credentials are obfuscated, and then sent over the network.

Securiteam: [NEWS] Apple AirPort Administrative Password Obfuscation

The authentication credentials, a password with a maximum length of 32 characters, are XOR'd against a predefined key. When sent over the network, the password is sent out in a 32 byte fixed block. @stake was able to determine the key by setting a one-character password and monitoring the network traffic. This revealed 31 bytes of the XOR 'key'. The final byte can be obtained by XORing the obfuscated first byte against the first character of the plaintext password.

If an AirPort is administered over the Ethernet interface or via an insecure (non-WEP) wireless connection, an anonymous attacker that can sniff the network can obtain administrative access to the AirPort. If WEP is enabled, then the attack is limited to WEP authenticated attackers.

Vendor Response:

The recommendation is to administer the AirPort Base Station either via a wired connection or via a WEP-protected wireless connection.

Recommendation:

The only way to securely administer the AirPort Base Station is by connecting to it via a crossover cable. In environments where this is not practical, it is advised that the AirPort Base Station be managed through the Ethernet network, and not the wireless network.

ADDITIONAL INFORMATION

The original advisory can be downloaded from:

<<http://www.atstake.com/research/advisories/2003/a051203-1.txt>>
<http://www.atstake.com/research/advisories/2003/a051203-1.txt>

The information has been provided by <mailto:advisories@atstake.com>
@stake Advisories Jeremy Rauch and <mailto:daveg@atstake.com> Dave G..

=====

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.