

[NEWS] Linksys Routers Found to be Vulnerable to SNMP Issues

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0054.html>

From: support@securiteam.com

Date: 01/13/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 13 Jan 2002 23:33:16 +0100 (CET)

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.

Linksys Routers Found to be Vulnerable to SNMP Issues

SUMMARY

<<http://www.linksys.com/>> Linksys DSL routers suffer from serious information leakage problems, as well as a potential opening to be used as a DDoS initiator.

DETAILS

Vulnerable systems:

BEFN2PS4 (EtherFast Cable/DSL Router & Voice with 4-Port Switch)

BEFSR81 (EtherFast Cable/DSL Router with 8-Port Switch) (confirmed version 2.37)

Immune systems:

BEFSR81 version v2.38.1

Querying the mentioned devices with the default community of 'public' causes them to set the address that queried as their snmptrap host, dumping traffic such as the following to that address:

Enterprise Specific Trap (1) Uptime: 2 days, 19:00:23.36,
enterprises.3955.1.1.0 = "@out 192.168.1.200 ==> 24.254.60.13[110]."

Securiteam: [NEWS] Linksys Routers Found to be Vulnerable to SNMP Issues

```
Enterprise Specific Trap (1) Uptime: 2 days, 19:00:23.36,
enterprises.3955.1.1.0 = "@out 192.168.1.200 ==> 216.120.8.23[5632]."
Enterprise Specific Trap (1) Uptime: 2 days, 19:00:23.36,
enterprises.3955.1.1.0 = "@out 192.168.1.200 ==> 216.120.8.3[5632]."
Enterprise Specific Trap (1) Uptime: 2 days, 19:00:23.36,
enterprises.3955.1.1.0 = "@out 192.168.1.200 ==> 216.120.8.4[5632]."
Enterprise Specific Trap (1) Uptime: 2 days, 19:00:23.36,
enterprises.3955.1.1.0 = "@out 192.168.1.200 ==> 216.120.8.5[5632]."
Enterprise Specific Trap (1) Uptime: 2 days, 6:04:38.11,
enterprises.3955.1.1.0 = "-->[U]Send OP: ^ps_status_q
15049C0DFC9B03166D55EA30474D04FB 9218583272 a .."
Enterprise Specific Trap (1) Uptime: 2 days, 6:04:38.11,
enterprises.3955.1.1.0 = "<--[U]Recv __:
^ps_status_r.15049C0DFC9B03166D55EA30474D04FB.\".\".0.."
```

It looks like a combination of debugging information as well as traffic logging; many customers never use the configuration page, let alone change the SNMP communities. To make matters worse, Linksys refuses to distribute an MIB for the device, which is not surprising considering the SNMP implementation on the device is rather broken (it goes into a continuous loop).

Further, with the correct community string you could enumerate values, determine the internal network addressing, etc, and even add forwarding rules to access services on internal hosts. When a change is made, the trick is to find the SNMP var that acts as the switch to save the new config values and recycle with the new values. Some poking and some Linksys MIBS found on the Internet id'd/confirmed the software switch as: 1.3.6.1.4.1.3955.3.1.6.0 Integer valued ... set to '1' to save new values/recycle.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:poptix@techmonkeys.org>> Matthew S. Hallacy and <<mailto:cyberiad@nmrc.org>> The Cyberiad.

=====

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.

Securiteam: [NEWS] Linksys Routers Found to be Vulnerable to SNMP Issues

- *Previous message:* support@securiteam.com: "[NEWS] Mail.com Cross Site Scripting Vulnerability"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)