

[NEWS] Linksys WET11 DoS (MAC address)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0124.html>

From: support@securiteam.com

Date: 10/25/02

From: support@securiteam.com

To: list@securiteam.com

Date: 25 Oct 2002 14:42:29 +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

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 WET11 DoS (MAC address)

SUMMARY

The Linksys WET11 is an Ethernet to 802.11b bridge. It can bridge a single host, or an entire network (Up to 50 machines). A security vulnerability in the product allows an attacker to send an arbitrary UDP packet causing it to crash.

DETAILS

Analysis:

When configuring a WET11, you have to run their Windows application to do the initial configuration, which is configured entirely by UDP broadcasting. The first thing the software does is probe for devices on the network by broadcasting to port 4000 of 255.255.255.255:

Packet Analysis:

Probe Packet:

<UDP headers snipped>

16 bytes:

87 65 43 21 11 00 00 01 /* This data isn't clear.. Everything but the 6th byte

is identical to the first 8 bytes of the response

Securiteam: [NEWS] Linksys WET11 DoS (MAC address)

```
packet */
a0 00 0d c9 e7 7c /* MAC Address of your machine */
00 00 /* NUL */

Response Packet:
<UDP headers snipped>
120 bytes:

87 65 43 21 11 10 00 01 /* Everything but the 6 byte is the same as the
first 8 in the Probe packet */
a0 00 0d c9 e7 7c /* MAC address of the requesting machine */
00 06 25 02 e4 71 /* MAC address of the WET11 */
45 53 33 30 30 62 /* Ascii: ES300b */
00 /* NUL */
10 6c 69 6e 6b 73 79 73 /* Ascii: linksys */
00 00 00 00 00 00 00 00 /* NUL */
00 00 00 00 00 00 00 00 /* NUL */
00 00 00 00 00 00 00 00 /* NUL */
00 00 /* NUL */
06 10 0e c0 a8 01 e1 /* unknown data, can be removed */
```

```
4c 69 6e 6b 73 79 73 20 57 45 54 31 31 /* SSID of unit, Default is
"Linksys WET11" */
```

```
00 00 00 00 00 00 00 00 /* NUL */
00 00 00 00 00 00 00 00 /* NUL */
00 00 00 00 /* NUL */
ff ff ff 00 /* Netmask 255.255.255.0 */
c0 a8 01 01 /* 192.168.1.1 (Default gw. The
unit default IP is 192.168.1.225) */
a6 e7 94 7f 8c 4b 9a ec /* This data changes on every response.. */
a5 13 87 /* This data changes on every response.. */
```

If you replay the response packet to the broadcast (Or modify the Destination address in the header to the actual unit IP), the unit crashes right away. At this point you have to hard cycle the unit.

You don't really have to replay to the packet (it's just an easy way of doing it) because the actual problem is the unit doesn't know what to do when Source MAC in the DLC header is the same as it's own. All you have to do is forge a packet to a broadcast address, or directly to the unit, using its MAC in the Ethernet frame, and the unit will crash. Netmask only tested this vulnerability with UDP.

Exploiting:

As it says above, forge its MAC in the DLC header, and hit it with a packet, and it's gone.

ADDITIONAL INFORMATION

Securiteam: [NEWS] Linksys WET11 DoS (MAC address)

The original advisory can be downloaded by going to:
<<http://www.enzotech.net/advisories/linksys.wet11.txt>>
<http://www.enzotech.net/advisories/linksys.wet11.txt>

The information has been provided by <<mailto:netmask@enZotech.net>>
netmask.

=====

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: "[NT] BRS WebWeaver Web Server Protected File Access Vulnerability"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)