

[Full-disclosure] Cisco Linksys WET11 Password Resetting Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-04/0148.html>

From: Kristian Hermansen (khermansen_at_ht-technology.com)

Date: 04/07/05

To: full-disclosure@lists.grok.org.uk

Date: Thu, 07 Apr 2005 03:13:32 -0400

=====
=====Analysis=====

Cisco's Linksys WET11 ethernet bridge product is vulnerable to password resetting based on GET fields in a URL directed at the device. The change password utility provided on the device uses GET to send an obfuscated password as the argument to the `changepw.html` page. The field that holds the password is named `data`. Here's what the URL looks like when the user tries to change the password to "admin":

<http://x.x.x.x/changepw.html?data=XVQsZV3.....>

The encoding of passwords is quite predictable, and I now show some examples of the passwords "a" through "h":

<http://x.x.x.x/changepw.html?data=XP.....>
<http://x.x.x.x/changepw.html?data=Xf.....>
<http://x.x.x.x/changepw.html?data=Xv.....>
<http://x.x.x.x/changepw.html?data=Y.....>
<http://x.x.x.x/changepw.html?data=YP.....>
<http://x.x.x.x/changepw.html?data=Yf.....>
<http://x.x.x.x/changepw.html?data=Yv.....>
<http://x.x.x.x/changepw.html?data=Z.....>

This doesn't really matter, since if you are already on the network and can sniff packets, you can just base64 decode the basic auth strings flying by. However, I suggest you change the password blindly on this device using the following:

<http://x.x.x.x/changepw.html?data=-.....>

This will create a blank password and allow you to login without knowing the old one. There is no verification when you change the password. In the newest version 1.5.4 of the firmware for the WET11 v1 device, however, someone must have logged in recently (timeout is `_LONG_` though)

Full-Disclosure: [Full-disclosure] Cisco Linksys WET11 Password Resetting Vulnerability

to allow for this attack (ie. it will request the old password). In this scenario, just have them log in to check their settings, and a few minutes later, blank the password.

=====
===Implications===
=====

This attack allows anyone to reconfigure the IP address of the device and change any settings that the device allows. In the latest v1 revision 1.5.4 of the firmware the old password must have been supplied recently to execute the attack.

=====
=====Affected=====

Tested on Linksys WET11 v1 (1.5.4)
Note: older versions may be affected++
Note: WET11 v2 not tested, but may be vulnerable as well

=====
=====Solution=====

Upgrade to the latest firmware to deter blind password resetting. Be aware that there is still no old password authentication when changing the password even in 1.5.4.
<http://www.linksys.com/download/firmware.asp>

--
Kristian Hermansen <khermansen@ht-technology.com>

Full-Disclosure - We believe in it.
Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>
Hosted and sponsored by Secunia - <http://secunia.com/>