

[NEWS] LG Electronics LG3100p Router Multiple Security Issues (DoS)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0110.html>

From: support@securiteam.com

Date: 08/27/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 27 Aug 2002 22:14:31 +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.

LG Electronics LG3100p Router Multiple Security Issues (DoS)

SUMMARY

LG Electronics LR3100p is a small WAN router, with two WAN interfaces and one Ethernet. It comes with no access lists defined, which enables administrator to connect to port 23/tcp (telnet). IP stack of LR3100p has several bugs that can be exploited via the network to effectively cause the product to misbehave (allowing attackers to cause a denial of service attack).

DETAILS

Vulnerable systems:

Versions up to and including 1.30 are vulnerable to all bugs mentioned.

Release 1.50 is vulnerable only to first and third bug.

Immune systems:

Version 1.52 fixes just issue number two.

Details:

When configured without access lists protecting port 23, the LR3100p is vulnerable to at least three bugs.

Securiteam: [NEWS] LG Electronics LG3100p Router Multiple Security Issues (DoS)

(1) Denial of service attack on Telnet port:

First is exploitable without any access to user account on the router. The only thing that needed is access to port 23/tcp. If the router is provided with a constant data stream (can be any characters, both randomized and text-only input were used during testing) coming to that port, the route will reboot, usually with no message.

(2) NMap causes denial of service (e.g. Fingerprinting):

Second bug is applicable only to software revisions up to and including 1.30. A few packets generated via simple scanning (for example nmap with '-O' option) can result in a reboot of the router with following message:
Exception 1400 at IP 12afc4

(3) Garbage password buffer denial of service:

Third bug is directly in the telnet service, when it checks for passwords. The same technique with random data stream is used, however a few ENTER characters should be sent before the stream is sent, this is done in order to overcome the router's primary prompt waiting for the ENTER key to be pressed. The stream's length was measured to be at about 40kB. As before the router reboots without any message.

Vendor response:

The vendor representative was informed about the vulnerabilities on 2002-04-18, and LG has recently released a 'fixed' release 1.52 that, however, is still vulnerable to first and third bug. They were notified of the fact, but no response has been received.

ADDITIONAL INFORMATION

The original advisory can be accessed by going to:

<<http://mr0vka.eu.org/docs/advisories/lg-3100p-2002-04-18.txt>>
<http://mr0vka.eu.org/docs/advisories/lg-3100p-2002-04-18.txt>

The information has been provided by <<mailto:lbromirski@mr0vka.eu.org>>
Lukasz Bromirski.

=====

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] LG Electronics LG3100p Router Multiple Security Issues (DoS)

- **Previous message:** support@securiteam.com: "[NEWS] Light Vulnerable to Remotely Exploitable Arbitrary Code Execution"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)