

[NEWS] ELSA Lancom 1100 Office Security Problems

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0002.html>

From: support@securiteam.com

Date: 01/02/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 2 Jan 2002 08:07:28 +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.

ELSA Lancom 1100 Office Security Problems

SUMMARY

Phoenix Sistemi Security reports several security problems in

<http://www.elsa.com/international/europe/produkte/netzwerk/lc_1100_off.htm> ELSA Lancom 1100 Office.

An attacker can steal the RAS password, change routing tables, and place a modified firmware to sniff data.

DETAILS

Vulnerable systems:

ELSA Lancom 1100 Office

ELSA Lancom 1100 Office has to be configured by browser on an HTTP connection over port 80 on the router IP. An intruder can connect with a browser to the router ip (Intranet or Internet) and change the routing tables or steal the RAS password that is stored in a field covered with asterisks. The passwords are stored in clear text and can be seen by editing the html source.

That is not all; the upgrade of the firmware could be done remotely just going in its appropriate page placed in the configuration table, and an attacker can upgrade a customized firmware that will sniff all the data passing by the router.

Securiteam: [NEWS] ELSA Lancom 1100 Office Security Problems

Solutions & Recommendations:

Changing the configuration port is a good idea to prevent random attacks. Another good idea would be to give access privileges to first-time configuration just to an internal ip addresses. The RAS password should be stored in a file different from the html, or that part of configuration could be done with a JavaScript.

An easy user-side solution could be to install a firewall with appropriate rules, so that no one from the Internet would have access to it.

ADDITIONAL INFORMATION

The information has been provided by <mailto:security@phx.it> Davide Del Vecchio.

=====

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] Cherokee Webserver Directory Traversal and Elevated Privileges Vulnerabilities"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)