

[NEWS] Lucent Brick VPN Firewall Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0130.html>

From: support@securiteam.com

Date: 07/30/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 30 Jul 2002 08:23:16 +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.

Lucent Brick VPN Firewall Multiple Vulnerabilities

SUMMARY

The

<<http://www.lucent.com/products/subcategory/0..CTID+2017-STID+10080-LOCL+1.00.html>> Lucent Brick VPN Firewall is a layer 2, NCSA, US Army, and US National Security Agency (NSA) Approved/Certified Firewall that operates on Inferno, an Embedded Operating System. "Brick" devices come in many sizes from the SOHO Brick 20 to the Enterprise 1000 (GiG). Three design flaws in the firewall allows attackers to interrupt the connection between the firewall and its management station, cause the firewall to forward ARP packets regardless of any firewall rules, and to easily identify the firewall product remotely.

DETAILS

Vulnerable systems:

* Lucent LSMS version 5.5 (Lucent Brick, Bridging VPN Firewall)

The Brick suffers from several design failures in handling of the ARP protocol.

1. It is possible to interrupt any connection between the Brick and critical devices such as the LSMS (Brick Management Server) by binding the IP Address of the device in question to the attackers interface and

Securiteam: [NEWS] Lucent Brick VPN Firewall Multiple Vulnerabilities

"pinging" the Brick or any address behind it. The Brick will immediately update its ARP cache and drop the connection, no matter where the attacker is located (internal/outside segment). This requires the "Floating MAC" setting to be turned on.

2. The Brick will forward any ARP request and response across all interfaces, regardless of the existing firewall rules.

3. All Bricks are identifiable during reconnaissance using the most basic of techniques (pinging all addresses in segment). The device that sends ARP requests for the attacker IP address is the Brick.

Example:

1. # man ping
2. # man arp
3. # for i in `cat ipaddresses.txt`; do ping \$i; done

Vendor status:

06/28/02 Reply to inquiry regarding "who to notify"
06/29/02 Initial Notification to Brick team *Note-Initial notification by phenoelit includes a cc to cert@cert.org by default
07/02/02 Acknowledgement of receipt by Lucent Brick team
07/06/02 Weekly follow-up by central POC at Lucent (Right on Time)
07/08/02 Additional tech-discussions
07/19/02 Notification of intent to post publicly in approximately 7 days.
07/25/02 Notification that due to personnel changes at Lucent, our POC has changed. The new person is supposed to be contacting us.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:fx@phenoelit.de>> FX and <<mailto:kim0@phenoelit.de>> kim0.

=====

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] Linux 'util-linux' chfn Local Root Vulnerability"

Securiteam: [NEWS] Lucent Brick VPN Firewall Multiple Vulnerabilities

- *Messages sorted by:* [date] [thread] [subject] [author] [attachment]