

[NEWS] Novell Border Manager Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0042.html>

From: support@securiteam.com

Date: 05/08/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 8 May 2002 18:26:09 +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.

Novell Border Manager Multiple Vulnerabilities

SUMMARY

Multiple vulnerabilities identified in Novell Border Manager 3.6. During a brief look at Novell Border Manager 3.6, there have been identified three issues within the product. The vulnerabilities will cause the handling NLM to abend, and in some cases result in a DOS of the Novell server.

DETAILS

Vulnerable systems:

- * Border Manager version 3.6 SP 1a

The first vulnerability is within the FTP-proxy server of BM 3.6. After issuing the connection request to the proxy an attacker could send a couple of messages of random data, which would cause the server to stop responding to TCP/IP for a while. The server will then start answering TCP/IP traffic again after 10 to 20 seconds. If this is repeated for ten times or so, our test environment stop responding to TCP/IP altogether, and the server had to be rebooted to regain full function ability.

The second vulnerability is in the IP/IPX gateway on tcp port 8225. If one would send approximately two megabytes of random data to this port, the

Securiteam: [NEWS] Novell Border Manager Multiple Vulnerabilities

NLM ipipxgw.nlm will abend.

The third vulnerability is in the RTSP proxy running on port 9090. One could cause the proxy.nlm to abend by simply connecting to the port, issuing the command "GET" followed by six enters.

Solution:

Filter incoming connections to the ports 21, 8225 and 9090. As soon as patches become available, apply them.

Vendor status:

Novell was contacted 20020412 and have been unable to reproduce the issues up until today.

ADDITIONAL INFORMATION

The information has been provided by
<mailto:patrik.karlsson@se.pwcglobal.com> Patrik Karlsson &
<mailto:jonas.landin@ixsecurity.com> Jonas Ländin.

=====

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: "[NEWS] The Netware FTP Server Contains a DoS vulnerability"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)