

[NT] Avirt Gateway Telnet Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0118.html>

From: support@securiteam.com

Date: 01/24/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 24 Jan 2002 22:42:51 +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.

Avirt Gateway Telnet Vulnerability

SUMMARY

<<http://www.avirt.com/>> Avirt specializes in the development of (inter-)networking and sharing technologies. As such, it maintains the SOHO and Gateway proxy product lines.

Recently, the SNS research team published two advisories in regards to these products, after which they were informed of at least one other buffer overflow vulnerability in Avirt's Gateway product line

DETAILS

Vulnerable systems:

Avirt Gateway version 4.2

The Avirt Gateway technology contains, amongst others, a telnet proxy. Due to a failure to check for length of the input served to this proxy, a buffer overflow condition exists which could be exploited to execute arbitrary code on the target system.

To exploit this flaw an attacker would have to connect to the telnet proxy and at the "Ready>" prompt pass it a buffer of >2000 bytes. The service will die and the EIP is overwritten.

Securiteam: [NT] Avirt Gateway Telnet Vulnerability

All Avirt's Gateway products run as a NT system service by default.

Solution:

Vendor has been notified at the time this message went out.

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:vuln-dev@labs.secureance.com>> Strumpf Noir Society.

=====

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: "[NT] Citrix NFuse Information Leak"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)