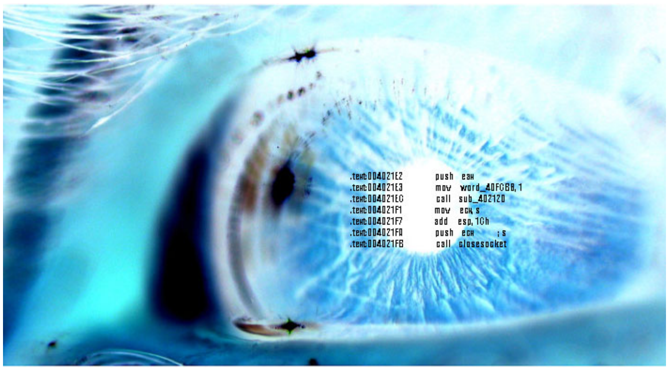
CIRT

Danish Computer Incident Response Team

Security advisory

OpenConnect WebConnect 6.4.4 and 6.5 (Win32 version)



```
.text:004021E2        push  eax
.text:004021E3        mov   word_40FCB8,1
.text:004021EC        call  sub_402120
.text:004021F1        mov   ecx,s
.text:004021F7        add   esp,10h
.text:004021FA        push  ecx       ;s
.text:004021FB        call  closesocket
```

Discovered
by Dennis Rand
advisory@cirt.dk
http://www.cirt.dk

21-02-2005

Table of contents

Introduction

Problem

The installation has been made on a Windows 2000 server running with the latest patch level.

The WebConnect 6.4.4 and 6.5 contains several vulnerabilities such as:

- Denial of Service when requesting an DOS Device in Path Name
- Reading of files outside webroot (Directory traversal)

Who are OpenConnect

http://www.openconnect.com/company/index.jsp
OpenConnect Systems is the premier supplier of secure Mainframe-to-Web solutions for Global 2000 organizations. Our Mainframe2Web Secure Solutions Series provides companies with cost effective, secure access to critical business information and applications within mainframes. By providing our customers, partners and employees with secure access to mainframe data, organizations can significantly increase productivity, information sharing and revenue generating opportunities.

Our Mainframe2Web Secure Solutions Series consists of Secure Access Solutions (WebConnect, WebConnect SSO), Mainframe2Web Development Tools (eXtremeVista and Visual 3270) and Web Services Development Tools (xmlConnect). Our products are distributed in over 60 countries and used by more than 60% of Fortune 100 companies.

What is WebConnect

WebConnect is client-server based software that provides secure browser based emulation to mainframe, midrange and UNIX systems. WebConnect enables enterprise organizations to provide suppliers, partners and employees with secure access to vital applications and information. Enterprises increase productivity and profits, and retain all the advantages of secure host connectivity to new and existing applications in "real-time."

Because WebConnect is non-intrusive, it provides secure SSL encrypted information migration and access without requiring modification to the host. With its patented secure, "persistent connectivity" technology, only WebConnect is capable of supporting tens of thousands of concurrent browser-based users.

http://www.openconnect.com/solutions/webconnect.jsp

Timeline of public disclosure

- 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
  - 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
  - VU#628411 / CAN-2004-0465
- 14-02-2005 Public Disclosure delayed due to request from vendor
- 21-02-2005 Public Disclosure

Contact information

The following vulnerability were discovered by Dennis Rand at CIRT.DK
Questions regarding this issue should be directed to:

Dennis Rand
advisory@cirt.dk

File description and MD5 checksum

MD5 software used

Filename:	md5sum.exe
Comments:	Modified from the version originally developed by Ulrich Drepper <drepper@gnu.ai.mit.edu>
Company name:	GMG Systems, Inc.
Product name:	Forensic Acquisition Utilities
Product version:	1.0.0.1026
File version:	2.0.1.1032
MD5 checksum:	607be2b261c516a5c5469314445ab2f2

WebConnect 6.4.4

Installation files:

Filename:	WC6_4_4-win32-ssl-rsa-domestic.exe
MD5 checksum:	35f7e73b2ac96cb1078c8baf57c6c070

Service files:

Service Name:	WebConnect WC6.4.4
Filename:	WCD.EXE
MD5 checksum:	c32d1b91fd0c8ba176df26bd0ae06e08

HTML files

Filename:	jretest.html
MD5 checksum:	368bb580bb8b66ee262619bd035d5841

WebConnect 6.5

Installation files:

Filename:	NT65DE.exe
MD5 checksum:	7f945a7c5636b7b371a65d35dfac842d

Service files:

Service Name:	WebConnect WC6.5
Filename:	WCD.EXE
MD5 checksum:	52840846ba853041a1a1f389db594627

Filename:	libhttp.dll
MD5 checksum:	6b66f2881f20143d16193fe4f67a6444

Short description of the vulnerabilities

Requesting "DOS Device in Path Name" Denial of Service

When requesting a DOS device in the URL the server will stop responding to any further requests before a manual restart of service has been made.
This attack can be preformed on both the client website and the administration interface.

Vulnerable versions:

- WebConnect 6.4.4 (Possible previous versions)
- WebConnect 6.5

CERT response:
VU#552561
CAN-2004-0466

Reading of files outside webroot (Directory traversal)

When sending a specially crafted request to the server it is possible to read files outside the webroot. Since the service as default runs with system rights, this could give access to the entire partition that WebConnect are installed on.

Vulnerable versions:

- WebConnect 6.4.4 (Possible previous versions)

CERT response:
VU#628411
CAN-2004-0465

Technical details of the vulnerabilities

Requesting "DOS Device in Path Name" Denial of Service

The problem exhibits itself when requesting an URL that includes reserved MS-DOS devices. These represent devices such as the first printer port (LPT1) and the first serial communication port (COM1). Sample reserved MS-DOS device names include:

- AUX
- CON
- PRN
- COM1
- LPT1

Default open web-ports:

2080	HTTP - Client website
2443	HTTPS - Client website
4270	HTTP - Administration interface
4443	HTTPS - 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

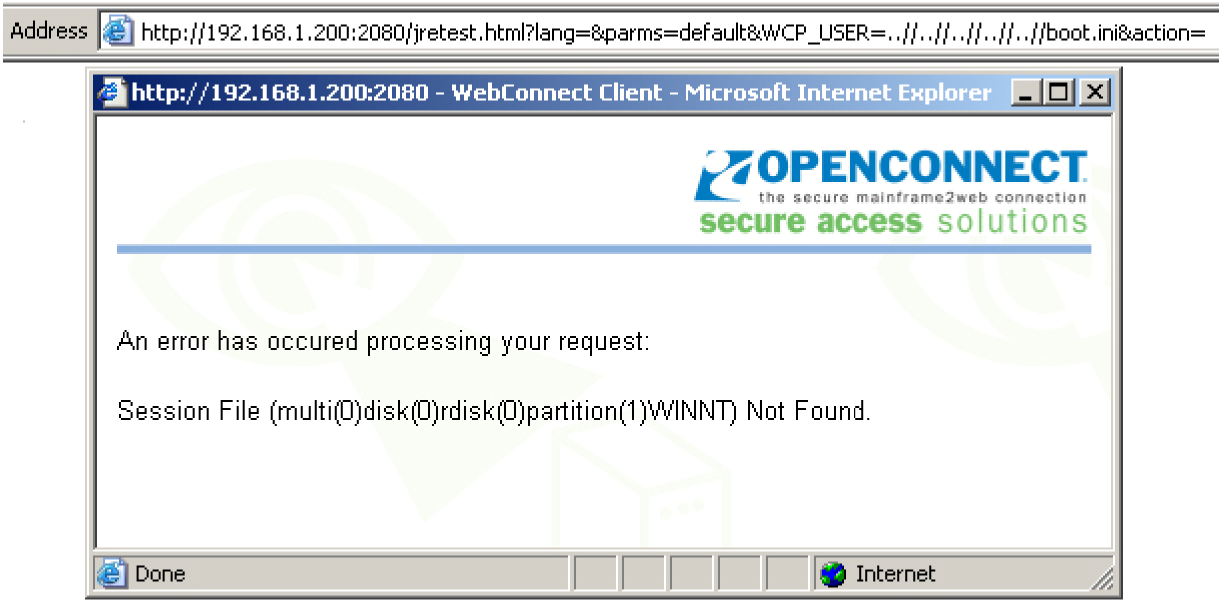
Vulnerable versions:

- WebConnect 6.4.4 (Possible previous versions)
- WebConnect 6.5

Reading of files outside webroot (Directory traversal)

The file jretest.html are vulnerable to reading files from outside the webroot, this seems only possible if the "parms" has to be set to "default".
This problem shows that the file does not properly input sanitize

Proof-of-concept:
http://target:2080/jretest.html?lang=&parms=default&WCP_USER=..//..//..//..//..//boot.ini&action=



Address
http://192.168.1.200:2080/jretest.html?lang=&parms=default&WCP_USER=..//..//..//..//..//boot.ini&action=
http://192.168.1.200:2080 - WebConnect Client - Microsoft Internet Explorer
OPENCONNECT
the secure mainframe2web connection
secure access solutions
Done
Internet

An error has occured processing your request:

Session File (multi(0)disk(0)rdisk(0)partition(1)WINNT) Not Found.

Vulnerable versions:

- WebConnect 6.4.4 (Possible previous versions)

Corrective actions

Upgrade to OpenConnect WebConnect version 6.5.1 or later to solve the security issues specified in this advisory.

There has also been made a fix for version 6.4.5
Checksum: 17e1e77b083369ba38e12dd636835f12 (wcd.exe)

Customers go through our support organization to obtain updates so there won't be a webpage for the updates.

Disclaimer

The information within this document may change without notice.
Use of this information constitutes acceptance for use in an "AS IS" condition.

There are NO warranties with regard to this information.

In no event shall I be liable for any consequences or damages, including direct, indirect, incidental, consequential, loss of business profits or special damages, arising out of or in connection with the use or spread of this information.

Any use of this information lies within the user's responsibility. All registered and unregistered trademarks represented in this document are the sole property of their respective owners.