

[NEWS] Directory Traversal Vulnerabilities in FTP Clients

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-12/0032.html>

From: support@securiteam.com

Date: 12/11/02

From: support@securiteam.com

To: list@securiteam.com

Date: 11 Dec 2002 11:26:21 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Directory Traversal Vulnerabilities in FTP Clients

SUMMARY

FTP clients, including those that may be embedded in web clients, can be vulnerable to certain directory traversal attacks by modified FTP servers. If successful, the attacks could allow the server to overwrite or create arbitrary files outside of the client's working directory, subject to file/directory permissions and the privilege level of the client.

Multiple clients are affected. See "Test Results" for the list of clients.

DETAILS

Vulnerable:

Product ../ ..\ C: /path ...

wget 1.8.1 yes no no yes{4} no

wget 1.7.1 yes no no no{2} no

OpenBSD 3.0 FTP yes no{1} no{1} yes no

Solaris 2.6, 7 yes no no yes no

The ftp command on SGI systems is also subject to one or more flavors of directory traversal attacks. However, details were not available at the

Securiteam: [NEWS] Directory Traversal Vulnerabilities in FTP Clients

time that this advisory was published.

Not Vulnerable:

Product ../ ..\ C: /path ...

Red Hat 7.1 no{3} no{3} no{3} no{3} no
Debian 2.4.16 no{3} no{3} no{3} no{3} no
NT SP5 command line no no no no no
XP command (no SP) no no no no no
lftp 2.6.2 no no{1} no{1} no no
NcFTP 3.1.4 no no no no no
Lynx 2.8.1 [FTP traversal not available]

Notes:

- {1} installed the file in the current directory
- {2} created subdirectories within the current directory
- {3} generated error message and/or stopped downloading
- {4} only with the `-nH` option ("Disable host-prefixed directories")

Other notes on wget:

- 1) "wget" was tested with the `-r` (recursive) option.
- 2) When provided with an FTP URL on the command line, it is subject to `"/"` traversal
- 3) If there's an FTP link within a web page, it will not follow the links, and is not subject to traversal
- 4) HOWEVER, if the `--follow-ftp` option is used, it is subject to `"/"` traversal
- 5) When both `--follow-ftp` and `-nH` are used, wget is also subject to `"/path"` traversal
- 6) wget 1.7.1 was not tested for the `-nH` absolute path issue, or for FTP URL's in web pages

Vendor response:

Vendors informed individually and through CERT/CC

Risk:

A malicious server could potentially overwrite key files to cause a denial of service or, in some cases, gain privileges by modifying executable files. The risk is mitigated because non-default configurations are primarily affected, and the user must be convinced to access the malicious server. However, web-based clients may be more easily exploited using server-side vulnerabilities such as XSS.

Verification:

The task would involve creating a malicious FTP server that would send filenames with `"/"` and other sequences as the result of a "LIST" request, or a "multiple GET" request. The client might then download these files into some parent directory.

Testing Methodology:

This methodology is a simplification of the PROTOS methodology as

Securiteam: [NEWS] Directory Traversal Vulnerabilities in FTP Clients

developed by the Oulu University Secure Programming Group [2], in which a test suite is developed for a particular protocol, and the suite is then used against specific implementations. The PROTOS methodology has proven effective in finding large numbers of vulnerabilities in many different products that implement standard networking protocols.

For a simple test suite, the "ftp4all" FTP server was modified to return filenames of various forms that might cause files to be created outside a client's working directory. ftp4all was chosen because it was easy to install and it allowed non-root users to run an FTP server on a port other than 21.

The files src/ftps/list.c, serverd.c, and transfer.c were changed to produce modified filenames, and to return the same test file for any filename that the client requests.

When a client sends a LIST or NLST command, the test server returns filenames containing the following sequences:

- "./" – classic traversal
- "/path" – an absolute pathname
- "..\" – backslash traversal pattern (Windows systems)
- "C:" – Drive letter traversal (Windows systems)
- "..." – "triple-dot" (Windows systems, equivalent to ../../)

When downloading a group of files using wildcards, the FTP client typically performs an "NLST" command, reads the list of files returned by the server, and uses those filenames to make individual requests.

Note that web clients may also be affected if they can process "ftp://" URLs.

Demonstration Session:

Following is a simulated session to demonstrate how a vulnerable client may behave.

```
CLIENT> CONNECT server
220 FTP4ALL FTP server ready. Local time is Tue Oct 01, 2002 20:59.
Name (server:username): test
331 Password required for test.
Password:
230-Welcome, test – I have not seen you since Tue Oct 01, 2002 20:15 !
230 At the moment, there are 0 guest and 1 registered users logged in.
```

```
CLIENT> pwd
257 "/" is current directory.
```

```
CLIENT> ls -l
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
total 1
```

Securiteam: [NEWS] Directory Traversal Vulnerabilities in FTP Clients

```
-rw-r----- 0 nobody nogroup 0 Oct 01 20:11 ...\\FAKEME5.txt
-rw-r----- 0 nobody nogroup 0 Oct 01 20:11
./../FAKEME2.txt
-rw-r----- 0 nobody nogroup 0 Oct 01 20:11 ../FAKEME1.txt
-rw-r----- 0 nobody nogroup 0 Oct 01 20:11
\\.\\FAKEME4.txt
-rw-r----- 0 nobody nogroup 0 Oct 01 20:11 ..\\FAKEME3.txt
-rw-r----- 0 nobody nogroup 0 Oct 01 20:11
/tmp/ftptest/FAKEME6.txt
-rw-r----- 0 nobody nogroup 0 Oct 01 20:11
C:\\temp\\FAKEME7.txt
-rw-r----- 0 nobody nogroup 54 Oct 01 20:10 FAKEFILE.txt
-rw-r----- 0 nobody nogroup 0 Oct 01 20:11 misc.txt
226 Directory listing completed.
```

CLIENT> GET *.txt

```
Opening ASCII data connection for FAKEFILE.txt...
Saving as "FAKEFILE.txt"
```

```
Opening ASCII data connection for ../../FAKEME2.txt...
Saving as "../../FAKEME2.txt"
```

```
Opening ASCII data connection for /tmp/ftptest/FAKEME6.txt...
Saving as "/tmp/ftptest/FAKEME6.txt"
```

[etc.]

If a client is vulnerable, it saves files outside of the user's current working directory.

Testing Notes:

For command-line FTP clients, the client was tested in the following fashion:

- log onto FTP server
- set no-interactive prompt
- perform "mget" (multiple GET) or equivalent command

In some cases, an FTP client would produce an error as soon as it encountered a suspicious filename, and skip the remaining filenames. Thus one could not be certain if the client was vulnerable to other filenames. If a client demonstrated this behavior, then the server was modified to send a single suspicious filename at a time, and the client would be executed multiple times.

Other variants of directory traversal sequences were not tested, as there were not sufficient resources to conduct such a comprehensive analysis in a timely fashion. See [3] for examples.

Securiteam: [NEWS] Directory Traversal Vulnerabilities in FTP Clients

It is possible that web clients may be vulnerable to the same type of issue from malicious HTTP servers, when the clients are used to automatically download web pages. However, this was not tested.

Test Results:

The following products were specifically tested by the author. Descriptions of this class of problem were reported to CERT/CC and major vendors. Most vendors did not report results back to the author. Consult your vendor, or the associated CERT vulnerability note, if your product is not listed here.

Patches, Workarounds, and Vendor Statements:

Workarounds:

Some clients may have one or more of the following features. If so, then enabling these features could notify the user if an attack occurs, and allow the user to take defensive action.

These features may be explicitly disabled if the client is being called from a script or other program that does not require user intervention.

- 1) The user may be able to set the client to prompt the user when an existing file is to be overwritten. This is typically a default behavior.
- 2) A command such as "runique" may be available to force the client to use a different filename instead of overwriting an existing file.

Sun FTP client:

Statement from Sun

We have investigated this directory traversal issue and do not think it is a bug.

The user has several means of protection against this issue.

1. By default prompting is turned on, so the user gets a chance to decide if they want a file returned by mget before it is downloaded. So files will not be overwritten without prompting the user.
2. When running as an ordinary user, UNIX access controls will stop system files being over written. If a user must run as root, care needs to be taken which would include not turning off interactive mode.
3. The user may run the "runique" command to force the Solaris ftp client to avoid overwriting files that already exist.

The Solaris ftp mget behaviour is consistent with other BSD derived ftp clients, for example on Linux and FreeBSD. Changing the existing behaviour will cause problems.

SGI FTP client:

SGI acknowledged the vulnerability via email and is likely to have a public acknowledgement near the time of this disclosure.

Securiteam: [NEWS] Directory Traversal Vulnerabilities in FTP Clients

OpenBSD:

Vendor statement (Theo de Raadt):

"I've forwarded the report to the person who copes with that stuff. I do not consider this all that serious."

wget:

Red Hat Linux has released advisory RHSA-2002:229 at:

<<http://www.redhat.com/support/errata/RHSA-2002-229.html>>

<http://www.redhat.com/support/errata/RHSA-2002-229.html>

The status of other Linux vendors was unknown at the time this advisory was published.

Research and Disclosure History:

The disclosure of this issue has been conducted in accordance with the Christey/Wysopal "Responsible Vulnerability Disclosure Process" draft, which has expired [8].

Since multiple vendors and products were affected, the research and disclosure history for this issue is extensive. The total amount of time required for research, vendor notification, and coordination is estimated to be 50 hours.

Research and General Notification:

Sep 25, 2002 – issue theorized

Sep 27, 2002 – modified FTP server created; initial tests

Oct 1, 2002 – notified vendor-sec with various responses

Oct 10, 2002 – sent update to CERT/CC

Oct 11, 2002 – CERT/CC reply

Dec 2, 2002 – notified CERT/CC of status

Dec 2, 2002 – set release date of December 10, notified all parties

Dec 5, 2002 – received CERT ID (VU#210409) for issue

Dec 9, 2002 – more edits

Dec 9, 2002 – CVE ID's sent to vendor-sec

Sun (CVE: CAN-2002-1345)

Sep 27, 2002 – Sun ftp client issue discovered

Sep 30, 2002 – Notified Sun

Sep 30, 2002 – CERT/CC notified of Sun issue

Oct 1, 2002 – initial response from Sun (within 1 day)

Oct 1, 2002 – provided fake FTP server to Sun

Oct 7, 2002 – additional info from Sun

Nov 18, 2002 – response from Sun; will not address issue, as other protections are already available

Dec 2, 2002 – suggested "vendor statement" to Sun

Dec 4, 2002 – Sun provides final statement

SGI (CVE: CAN-2002-1345)

Oct 1, 2002 – provided fake FTP server to SGI

Nov 5, 2002 – inquiry by SGI on release status

Nov 27, 2002 – SGI inquires about release date

Securiteam: [NEWS] Directory Traversal Vulnerabilities in FTP Clients

Dec 2, 2002 – response to SGI; set release to Dec 10?

Dec 9, 2002 – CVE candidate acquired, sent to SGI

OpenBSD (CVE: CAN-2002-1345)

Oct 1, 2002 – OpenBSD client issue discovered

Oct 1, 2002 – notified OpenBSD (deraadt@openbsd.org)

Dec 2, 2002 – second notification to OpenBSD

Dec 2, 2002 – response from Theo de Raadt (original message was lost)

Dec 2, 2002 – report forwarded to other OpenBSD maintainers

wget (CVE: CAN-2002-1344)

Note: notification and resolution of the wget issue was handled primarily through Mark Cox of Red Hat Linux, not the package maintainer.

Sep 30, 2002 – wget issue discovered

Sep 30, 2002 – notified Mark Cox (Red Hat) of wget issue

Oct 1, 2002 – found wget absolute path issue

Oct 2, 2002 – provided fake web server to Red Hat

Oct 6, 2002 – notified wget developer (hniksic@arsdigita.com)

Nov 7, 2002 – inquiry by Red Hat on release status for wget; still haven't heard back from hniksic@arsdigita.com, need to consider other options

Nov 25, 2002 – Red Hat notifies that wget patches are ready

Dec 2, 2002 – notification to wget developer; new email address found by Red Hat; developer is mostly inactive

Dec 9, 2002 – CVE ID acquired, sent to Red Hat

Other Activities

Oct 1, 2002 – provided fake FTP server to Solar Designer

Oct 1, 2002 – briefly tested lftp

Oct 9, 2002 – received report that ncftp is vulnerable to /abs/path in the -R option; checked 3.1.4, doesn't seem to be an issue – "-R /" is interpreted as / on local system, so all pathnames would be "legal"; no response to followup

ADDITIONAL INFORMATION

References:

[1] "security hole in mget (in ftp client)" mhpower@MIT.EDU Bugtraq mailing list August 5, 1997

<<http://marc.theaimsgroup.com/?l=bugtraq&m=87602746719482&w=2>

<http://marc.theaimsgroup.com/?l=bugtraq&m=87602746719482&w=2> OUSPG: Oulu University Secure Programming Group

[2] OUSPG: Oulu University Secure Programming Group

<<http://www.ee.oulu.fi/research/ouspg/index.html>>

<http://www.ee.oulu.fi/research/ouspg/index.html>

[3] "A 'straw man' vulnerability auditing checklist" Steve Christey

SecProg mailing list December 5, 2002

<<http://marc.theaimsgroup.com/?l=secprog&m=103911851613670&w=2>

<http://marc.theaimsgroup.com/?l=secprog&m=103911851613670&w=2>//cve.mitre.org/cgi-bin/cvename.cgi?name=CA

Securiteam: [NEWS] Directory Traversal Vulnerabilities in FTP Clients

[4] <<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1344>>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1344>

[5] <<http://www.kb.cert.org/vuls/id/210148>>
<http://www.kb.cert.org/vuls/id/210148>

[6] <<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1344>>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1344>

[7] <<http://www.kb.cert.org/vuls/id/210409>>
<http://www.kb.cert.org/vuls/id/210409>

[8] <<http://www.wiretrip.net/rfp/p/doc.asp/i2/d73.htm>>
<http://www.wiretrip.net/rfp/p/doc.asp/i2/d73.htm>

The information has been provided by <<mailto:coley@mitre.org>> Steve Christey.

=====

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.