

# [NT] FTPServer/X Response Buffer Overflow Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0100.html>

---

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

*Date:* 06/26/03

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

Date: 26 Jun 2003 19:49:37 +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)

-----  
FTPServer/X Response Buffer Overflow Vulnerability  
-----

## SUMMARY

<<http://www.mabry.com/ftpserv/index.htm>> Mabry's FTP/X ActiveX control provides easy, high-level access to the complete FTP client protocol (RFC 959). In addition to capturing server directory listings into a string array property, the new FTP/X also makes the results available as an ADO Recordset providing easy access to the various fields that a server returns. The FTP/X also has powerful built-in features to support debugging and non-standard servers using the Quote method. A vulnerability has been identified in FTPServer/X, which can be exploited by malicious people to cause a DoS (Denial of Service) on a vulnerable FTP server or potentially compromise it.

## DETAILS

Vulnerable ActiveX Controls:

\* FTPServer/X – FTP Server Control and COM Object version 1.00.046

\* FTPServer/X – FTP Server Control and COM Object version 1.00.045

## Securiteam: [NT] FTPServer/X Response Buffer Overflow Vulnerability

Vulnerable products:

- \* Simple FTPServer Example (included with FTPServer/X)
- \* Mollensoft FTP Server version 3.5.2 (formerly known as Hyperion)
- \* Hyperion FTP Server version 3.0.0 (updated version downloaded 10/04/2003)

Immune ActiveX Controls:

- \* FTPServer/X – FTP Server Control and COM Object version 1.00.047

The vulnerability is caused due to a boundary error, when the FTP Server returns responses, which include user input. The problem is that the allocated buffer (1024 bytes) may be overflowed due to an insecure use of the "wsprintf()" function.

When exploiting the vulnerability, the return address as well as a pointer stored in the register "ecx" can be overwritten with arbitrary values.

Before returning, the manipulated pointer is used as an argument to the function "InterlockedDecrement()" in "kernel32.dll", which may cause a vulnerable FTP server to crash.

The FTP service needs to be restarted manually before functionality is restored.

Since the return address also is overwritten, the vulnerability can potentially also be exploited to execute arbitrary code on a vulnerable system.

The following two examples exploit the vulnerability.

Exploit 1 (Supply between 995 and 1017 bytes to the USER command):

```
telnet [victim] 21
USER AAAA...[995-1017]...AAAA
```

The FTP Server will crash when the "331 Password required for %s" response is returned.

Exploit 2 (Supply a 991 to 1022 bytes long invalid command):

```
telnet [victim] 21
AAAA...[991-1022]...AAAA
```

The FTP Server will crash when the response "500 '%s': command not understood" is returned.

Please note that "Exploit 2" is the same issue as the one reported by Moran Zavdi at the beginning of April in Hyperion FTP Server 3.0.0. However, this was erroneously thought to be fixed in an updated version of Hyperion FTP Server 3.0.0.

Solution:

Mabry Software has fixed the vulnerability in FTPServer/X version

## Securiteam: [NT] FTPServer/X Response Buffer Overflow Vulnerability

1.00.047.

Mollensoft has issued Mollensoft FTP Server version 3.5.3, which uses the latest version of FTPServer/X.

If your FTP server uses the FTPServer/X component (look for "FTPServX.dll" / "FTPServX.ocx"), check to see if an updated version of the product has been made available.

### Vendor timeline:

10/04/2003 – Vulnerability discovered in Hyperion FTP Server.  
11/04/2003 – Vendor notified (support@mollensoft.com).  
22/04/2003 – Vendor contacted again requesting acknowledgment.  
22/04/2003 – Vendor confirms vulnerability and states that it will be fixed in version 3.5.2.  
26/04/2003 – Vendor releases version 3.5.2.  
28/04/2003 – Vulnerability still present in latest version. Vendor notified (support@mollensoft.com).  
29/04/2003 – Mabry Software notified (techsupport@mabry.com) since the vulnerability may be caused by a boundary error in FTPServer/X used in Hyperion/Mollensoft FTP Server.  
09/05/2003 – Vulnerability conclusively identified in FTPServer/X.  
09/05/2003 – Vendor notified again (techsupport@mabry.com).  
09/05/2003 – Vendor confirms vulnerability.  
03/06/2003 – Vendor releases updated version (1.00.046).  
04/06/2003 – Vulnerability still present in latest version. Vendor informed (techsupport@mabry.com).  
12/06/2003 – Vendor provides source code and asks for help in identifying the problem.  
16/06/2003 – Problem identified.  
17/06/2003 – Mabry Software releases updated version (1.00.047).  
22/06/2003 – Mollensoft releases updated version (3.5.3).  
24/06/2003 – Public disclosure.

### ADDITIONAL INFORMATION

The original advisory can be downloaded from:

<[http://www.secunia.com/secunia\\_research/2003-3/advisory/](http://www.secunia.com/secunia_research/2003-3/advisory/)>  
[http://www.secunia.com/secunia\\_research/2003-3/advisory/](http://www.secunia.com/secunia_research/2003-3/advisory/)

The information has been provided by <mailto:che@secunia.com> Carsten H. Eiram.

=====

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

Securiteam: [NT] FTPServer/X Response Buffer Overflow Vulnerability

=====  
=====

**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.