

[UNIX] wu-ftp fb_realpath() Off-by-One Bug

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0002.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/01/03

To: list@securiteam.com

Date: 1 Aug 2003 01:02:48 +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

Get Thawte's New Step-by-Step SSL Guide for Apache.

In this guide you will find out how to test, purchase, install and use a Thawte Digital Certificate on you Apache web server.

Throughout, best practices for set-up are highlighted to help you ensure efficient ongoing management of your encryption keys and digital certificates. Get you copy of this new guide now:

<http://ad.doubleclick.net/clk;5903117;8265118;i>

wu-ftp fb_realpath() Off-by-One Bug

SUMMARY

Wu-ftp FTP server contains remotely exploitable off-by-one bug. A local or remote attacker could exploit this vulnerability to gain root privileges on a vulnerable system.

DETAILS

An off-by-one bug exists in fb_realpath() function. An overflow occurs when the length of a constructed path is equal to the MAXPATHLEN+1 characters while the size of the buffer is MAXPATHLEN characters only. The overflowed buffer lies on the stack.

The bug results from misuse of rootd variable in the calculation of length of a concatenated string:

```
-----8<-----cut here-----8<-----
```

```
/*
```

```
 * Join the two strings together, ensuring that the right thing
```

```
 * happens if the last component is empty, or the dirname is root.
```

Securiteam: [UNIX] wu-ftp fb_realpath() Off-by-One Bug

```
*/
if (resolved[0] == '/' && resolved[1] == '\0')
    rootd = 1;
else
    rootd = 0;

if (*wbuf) {
    if (strlen(resolved) + strlen(wbuf) + rootd + 1 > MAXPATHLEN) {
        errno = ENAMETOOLONG;
        goto err1;
    }
    if (rootd == 0)
        (void) strcat(resolved, "/");
    (void) strcat(resolved, wbuf);
}
-----8<-----cut here-----8<-----
```

Since the path is constructed from current working directory and a file name specified as a parameter to various FTP commands attacker needs to create deep directory structure.

Following FTP commands may be used to cause buffer overflow:

```
STOR
RETR
APPE
DELE
MKD
RMD
STOU
RNTO
```

This bug may be non-exploitable if size of the buffer is greater than MAXPATHLEN characters. This may occur for example if wu-ftp is compiled with some versions of Linux kernel where PATH_MAX (and MAXPATHLEN accordingly) is defined to be exactly 4095 characters. In such cases, the buffer is padded with an extra byte because of variable alignment that is a result of code optimization.

Linux 2.2.x and some early 2.4.x kernel versions defines PATH_MAX to be 4095 characters, thus only wu-ftp binaries compiled on 2.0.x or later 2.4.x kernels are affected.

Impact:

Authenticated local user or anonymous FTP user with write-access could execute arbitrary code with root privileges.

Vendor Status:

June 1, 2003 security@wu-ftp.org has been notified
June 9, 2003 Request for confirmation of receipt sent to security@wu-ftp.org
June 11, 2003 Response received from Kent Landfield

Securiteam: [UNIX] wu-ftp fb_realpath() Off-by-One Bug

July 3, 2003 Request for status update sent
July 19, 2003 vendor-sec list notified
July 31, 2003 Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by <mailto:cliph@isec.pl> Wojciech Purczynski and <mailto:funkysh@isec.pl> Janusz Niewiadomski.

=====

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.