

[UNIX] Wu-FTPd SKEY Stack Overflow Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0112.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/26/03

To: list@securiteam.com

Date: 26 Oct 2003 16:18:33 +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>

Wu-FTPd SKEY Stack Overflow Vulnerability

SUMMARY

The Washington University FTP daemon (hereafter referred to as "wuftpd") is a replacement FTP server for POSIX systems. Wu-FTPd supports SKEY authentication to provide secure logins. However, the code that 'handles' this has an exploitable stack based buffer overflow. By providing specially crafted authentication credentials, it is possible to crash the daemon or execute user-supplied code, running with root privileges.

DETAILS

Vulnerable systems:

* Wu-FTPd version 2.6.2 (with SKEY support enabled)

A statically allocated buffer is filled using the `sprintf()` function in the `skey_challenge()` function (`src/ftpd.c`).

```
char *skey_challenge(char *name, struct passwd *pwd, int pwok)
{
    $
}
```

Securiteam: [UNIX] Wu-FTPd SKEY Stack Overflow Vulnerability

```
static char buf[128];
...
if (pwd == NULL || skeychallenge(&skey, pwd->pw_name, sbuf))
$
    sprintf(buf, "Password required for %s.", name);
else
sprintf(buf, "%s %s for %s.", sbuf,
pwok ? "allowed" : "required", name);
return (buf);
}
```

The variable *name is never subject to any boundaries checking. It is possible to write beyond the buf[] array, overwriting the return address of the function, modifying the path of execution flow.

Fix/Workaround:

To protect you from this vulnerability, disable SKEY support, or apply the following patch:

```
% diff -u ftpd.c fixed-ftp.c
--- ftpd.c 2001-11-29 17:56:11.000000000 +0100
+++ fixed-ftp.c 2003-10-20 20:43:58.000000000 +0200
@@ -1662,9 +1662,9 @@
     /* Display s/key challenge where appropriate. */

     if (pwd == NULL || skeychallenge(&skey, pwd->pw_name, sbuf))
-    sprintf(buf, "Password required for %s.", name);
+    snprintf(buf, 128-1, "Password required for %s.", name);
     else
-    sprintf(buf, "%s %s for %s.", sbuf,
+    snprintf(buf, 128-1, "%s %s for %s.", sbuf,
             pwok ? "allowed" : "required", name);
     return (buf);
 }
%
```

Vendor status:

Michael Hendrickx found this vulnerability in Wu-FTPd two weeks ago, and has been waiting for a response from the Wu-FTPd development team without any luck.

ADDITIONAL INFORMATION

The information has been provided by <mailto:michael@scanit.be> Michael Hendrickx.

=====

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: [UNIX] Wu-FTPd SKEY Stack 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.