

[UNIX] Multiple Overflows in Spider

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0055.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/16/03

To: list@securiteam.com

Date: 16 Sep 2003 18:26:18 +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>

Multiple Overflows in Spider

SUMMARY

ZetaLABs (Zone-H Research Laboratories) has discovered multiple overflows in the game spider, an application contained in the Debian GNU/Linux distribution. Two vulnerabilities in the product allow local attackers to gain elevated privileges by overflowing internal variables in the program (it is possible to gain group privileges 'games').

DETAILS

Vulnerable systems:

- * Spider version 1.1

Heap Overflow:

The first vulnerability is a heap overflow. We can see the vulnerable code in the "util.c" file:

```
char *
remove_newlines(str)
char *str;
{
char *newstr;
char *n;
extern char *getenv();
```

Securiteam: [UNIX] Multiple Overflows in Spider

```
/* pad it generously to provide for tilde expansion */
n = newstr = (char *)calloc((unsigned)(strlen(str) + 256), 1);
[...]
/* tilde expansion */
if (*str == '~') {
/* user */
if (*(str + 1) == '/') {
(void)strcpy(newstr, getenv("HOME")); /* strcpy() unchecked */
[...]
}
```

We can see that the `calloc()` functions allocate a standard amount of memory, therefore if we put in the HOME environment variable more than 256 and the length of str in bytes, the overflow will occur.

Buffer Overflow:

The second vulnerability is a buffer overflow. We can see the vulnerable code in the "vx_ui.c" file:

```
spider_defaults_objects *
spider_defaults_objects_initialize(ip, owner)
spider_windowl_objects *ip;
Xv_opaque owner;
{
spider_defaults_objects *obj=ip->defaults;
char buf1[256];
[...]
char *helphome;
extern char *getenv();
if (((helphome = getenv("OPENWINHOME")) ||
(helphome = getenv("XVIEWHOME"))) &&
(helphome != (char *)NULL)) {
sprintf(buf1, "%s/lib/help/spider", helphome); /* unchecked sprintf() */
[...]
}
```

As you can see, there is a buffer (buf1) that is assigned to the size of 256 bytes. Therefore, if we insert more than 256-16 bytes (the length of "/lib/help/spider" is 16 bytes) in the OPENWINHOME or in XVIEWHOME environment variables we can cause the overflow.

Both vulnerabilities can be exploited by a local attacker to gain "gid=games" privileges.

Solution:

It is possible to download a simple patch from here:

<http://www.zone-h.org/download/file=4941>

<http://www.zone-h.org/download/file=4941>.

ADDITIONAL INFORMATION

The original advisory can be downloaded from:

<http://www.zone-h.com/en/advisories/read/id=3049/>

<http://www.zone-h.com/en/advisories/read/id=3049/>.

Securiteam: [UNIX] Multiple Overflows in Spider

The information has been provided by <mailto:secfoc@email.it> Astharot.

=====

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.