

# [UNIX] Buffer Overflow in Liquidwar

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-09/0041.html>

---

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

**Date:** 09/16/03

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

Date: 16 Sep 2003 15:12:36 +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>

-----

Buffer Overflow in Liquidwar

---

## SUMMARY

ZetaLABs (Zone-H Research Laboratories) has discovered a buffer overflow in the game <<http://www.ufoot.org/liquidwar/>> Liquidwar, an application contained in the Debian GNU/Linux distribution.

## DETAILS

Vulnerable systems:

- \* Liquidwar version 5.4.5

We can see the vulnerable code here:

```
#define STARTUP_MAX_PATH_LENGTH 1000
[...]
char STARTUP_CFG_PATH[STARTUP_MAX_PATH_LENGTH];
[...]
static void set_path (void)
{
char home_path[512];
char *home_env;
if (exist_argument_value (IDENT_CFG))
strcpy(STARTUP_CFG_PATH,get_argument_str (IDENT_CFG));
else
```

## Securiteam: [UNIX] Buffer Overflow in Liquidwar

```
{
#ifdef ALLEGRO_UNIX
home_env=getenv("HOME");
strcpy(home_path,home_env); /* unchecked strcpy() */
strcat(home_path,"/");
#else
home_env="";
strcpy(home_path,home_env); /* unchecked strcpy() but not dangerous */
#endif
strcpy(STARTUP_CFG_PATH,home_path); /* unchecked strcpy() */
strcat(STARTUP_CFG_PATH,DEFAULT_CFG_PATH);
}
```

This vulnerability can be exploited by a local attacker to execute arbitrary code with gid=games privileges.

### Solution:

It's possible to download a simple patch here:  
<<http://www.zone-h.org/download/file=4943>>  
<http://www.zone-h.org/download/file=4943>.

### ADDITIONAL INFORMATION

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](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.