

# [UNIX] Buffer Overflow in Whois Client

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-08/0064.html>

---

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

**Date:** 08/24/03

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

Date: 24 Aug 2003 16:35:19 +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 Whois Client

---

## SUMMARY

Whois client is "a client to query the Whois servers, collecting data about internet domains". Zone-h Security Team has discovered a buffer overflow vulnerability in Whois client (all versions).

## DETAILS

By default, the Whois client is not setuid, therefore the bug is not exploitable locally. However, there are many CGI scripts, written in PHP/Perl, that use the Whois client. Therefore, it is possible to gain remote access to the server with web server privileges.

To test the buffer overflow:

```
astharot@astharot astharot $ whois -g `perl -e "print 'a'x2000"`
```

Solution:

There is a simple workaround. In the file whois.c find the line `sprintf(p--, "%c %s ", ch, optarg);`

And replace it with

```
snprintf(p--, sizeof(fstring), "%c %s ", ch, optarg);
```

Securiteam: [UNIX] Buffer Overflow in Whois Client

ADDITIONAL INFORMATION

The information has been provided by <mailto:gentiliem@tiscali.it>  
Ox6D6362@zone-h.org.

=====

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.