

# [UNIX] Sharity Cifslogin Buffer Overflow (Arguments)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0115.html>

---

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

*Date:* 06/24/02

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

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

Date: Mon, 24 Jun 2002 11:08:40 +0200 (CEST)

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.

-----

Sharity Cifslogin Buffer Overflow (Arguments)

---

## SUMMARY

<<http://www.obdev.at/Products/Sharity.html>> Sharity is a software package that runs on UNIX machines and allows you to mount shares exported by Windows (NT, 95, for Workgroups, etc.), OS/2, samba etc. in your filesystem. It is NOT an ftp-like client like the smbclient program distributed with Samba it really mounts the shares in your filesystem just as NFS does. Since the major release 2, Sharity supports browsing (like the Windows "Network Neighborhood") and has a GUI for dialogs and for the configuration. A security vulnerability in HP's provided version allows attackers to gain elevated privileges by overflowing an internal buffer.

## DETAILS

A security vulnerability in the product allows local users to overflow one of the parameters (-U, -D, -P, -S, -N, -u,) and cause the application to execute arbitrary code. Since the program is setuid root, elevated privileges can be gained.

In case that the attacker provide an overlong filename (for example, longer than 10000 bytes) for example parameter "-P", it would overflow a dynamic allocated buffer. The attacker could modify arbitrary memory

## Securiteam: [UNIX] Sharity Cifslogin Buffer Overflow (Arguments)

address (such as saved return address, and function pointer, etc.) with some features of malloc()/free() implementation by overwriting the border data structure of the next dynamic memory chunk.

Example:

```
$ id
uid=110(alex) gid=102(informix)
$

$ uname -a
HP-UX Lab02 B.11.11 U 9000/800 1613339393 unlimited-user license
$

$ ls -la /opt/cifsclient/bin/cifslogin
-rwsr-xr-x 1 root users 53248 Mar 28 2001 /opt/cifsclient/bin/cifslogin

$ /opt/cifsclient/bin/cifslogin -P `perl -e '{print "A"x10000}'`
Memory fault
```

Workaround:

Temporarily remove the suid root or sgid root attribute of cifslogin:  
# chmod a-s /opt/cifsclient/bin/cifslogin

Solution:

Apply patch that fixes, CIFS/9000 Server (SAMBA) allows malicious local users to overwrite arbitrary files and devices, patch number PHNE\_24164.

Vendor status:

Contact information:

e-mail: [sharity@obdev.at](mailto:sharity@obdev.at)

www: <http://www.obdev.at/>

Author: Christian Starkjohann <[cs@obdev.at](mailto:cs@obdev.at)>

Response:

Date Sat, 15 June 2002 8:54:01am

From Sharity Support <[sharity-support@obdev.at](mailto:sharity-support@obdev.at)> Add to address book

To <[alex\\_hernandez@ureach.com](mailto:alex_hernandez@ureach.com)>

The /opt/cifsclient/bin/cifslogin program is NOT part of Sharity. This is HP's CIFS client. HP has based this client on an old version of Sharity that they have licensed.

I will forward your report to the people at HP who are responsible for this software. I will give credits to you, of course.

Thanks for reporting this problem!

Regards, Christian.

---

Sharity Support, Objective Development.

Securiteam: [UNIX] Sharity Cifslogin Buffer Overflow (Arguments)

[sharity-support@obdev.at](mailto:sharity-support@obdev.at)

Contact information: [security-alert@hp.com](mailto:security-alert@hp.com) [secure@hpchs.cup.hp.com](mailto:secure@hpchs.cup.hp.com)

Response: Date Mon, 17 June 2002 2:40:18pm From HP S/W Security Team <[secure@hpchs.cup.hp.com](mailto:secure@hpchs.cup.hp.com)>  
Add to address book To [alex\\_hernandez@ureach.com](mailto:alex_hernandez@ureach.com)

Hello Mr: Hernandez,

Please read it, retrieve the patch, and apply it to your Lab02 11.11 installation. The patch can be retrieved \*without\* a support contract by registering with [itrc.hp.com](http://itrc.hp.com). (Registration is for simplified mailing list maintenance on our part. Without that – no patches can be retrieved.)

Yours Truly, WTEC HP S/W Security Team. --

ADDITIONAL INFORMATION

The information has been provided by <[mailto:alex\\_hernandez@ureach.com](mailto:alex_hernandez@ureach.com)> Alex Hernandez.

=====

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): "[UNIX] Interbase malloc() Security Issues (INTERBASE)"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)