

# [UNIX] Samba Arbitrary File Access Vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0015.html>

---

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

**Date:** 10/04/04

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

Date: 4 Oct 2004 14:18:16 +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>

-----

Samba Arbitrary File Access Vulnerability

---

## SUMMARY

<<http://www.samba.org/samba>> Samba is an Open Source/Free Software suite that provides seamless file and print services to SMB/CIFS clients.

Remote exploitation of an input validation vulnerability in Samba allows attackers to access files and directories outside of the specified share path.

## DETAILS

### Vulnerable Systems:

- \* Samba versions 3.0.2 up to but not including 3.0.7
- \* Sambe versions 2.2.9 up to but not including 2.2.12

### Immune Systems:

- \* Samba versions 3.0.7 and 2.2.12

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0815>>  
CAN-2004-0815

Each file and directory name passed into Samba is converted and checked

## Securiteam: [UNIX] Samba Arbitrary File Access Vulnerability

with the functions `unix_convert()` and `check_name()`. The main purpose of the `unix_convert()` routine is to convert names from the DOS namespace to Unix namespace. It calls `unix_clean_name()`, which in turn removes double slashes, leading `'./'` characters and `'..'` directory-traversal characters. `check_name()` does any final checks necessary to confirm the validity of the converted filename and calls `reduce_name()`, which in turn calls `unix_clean_name()` for a second time. The end result allows for an attacker to specify the realpath of any file on the computer.

### Example:

`./\\\\etc` is passed to `unix_clean_name()`. It becomes `./\\etc`. The leading slash is then trimmed off to make `./etc`. It is then passed to `unix_clean_name()` again. The resulting string is `/etc`, which is an absolute path on the system.

### Impact

Successful exploitation allows remote attackers to bypass the specified share restrictions to gain read, write and list access to files and directories under the privileges of the user. In situations where a public share is available, the attack can be performed by unauthenticated attackers.

An attacker does not need exploit code to exploit this vulnerability. The `smbclient` program can be used to request/write/list files using the `"get"`, `"put"` and `"dir"` commands, respectively.

### Vendor Status:

Upgrade to the listed versions of Samba which are immune to this problem.

The patch for Samba 2.x can be found at

<http://us4.samba.org/samba/ftp/samba-2.2.12.tar.gz>

<http://us4.samba.org/samba/ftp/samba-2.2.12.tar.gz>

The patch for Samba 3.x can be found at

[http://us4.samba.org/samba/ftp/patches/security/samba-3.0.5-reduce\\_name](http://us4.samba.org/samba/ftp/patches/security/samba-3.0.5-reduce_name)

[http://us4.samba.org/samba/ftp/patches/security/samba-3.0.5-reduce\\_name](http://us4.samba.org/samba/ftp/patches/security/samba-3.0.5-reduce_name)

### Disclosure Timeline

09/22/2004 Initial vendor notification

09/22/2004 iDEFENSE clients notified

09/22/2004 Initial vendor response

09/30/2004 Coordinated public disclosure

### ADDITIONAL INFORMATION

The information has been provided by

<mailto:customerservice@idefense.com> iDEFENSE Security Advisory.

=====

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:

Securiteam: [UNIX] Samba Arbitrary File Access Vulnerability

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.