



# CVE-2007-0454

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2007-0454
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2007-02-06 02:28:00 UTC
<b>Updated</b>	2018-10-16 16:32:00 UTC
<b>Description</b>	Format string vulnerability in the afsacl.so VFS module in Samba 3.0.6 through 3.0.23d allows context-dependent attackers

## Risk And Classification

**Problem Types:** CWE-134

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	alpha	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	arm	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	hppa	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	ia-32	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	ia-64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	m68k	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	mips	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	mipsel	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	ppc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	s-390	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	sparc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	alpha	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	amd64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	arm	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	hppa	All

Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	ia-32	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	ia-64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	m68k	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	mips	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	mipsel	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	ppc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	s-390	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	sparc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	alpha	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	arm	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	hppa	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	ia-32	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	ia-64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	m68k	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	mips	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	mipsel	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	ppc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	s-390	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.0	All	sparc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	alpha	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	amd64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	arm	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	hppa	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	ia-32	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	ia-64	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	m68k	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	mips	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	mipsel	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	ppc	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	s-390	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	3.1	All	sparc	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	2006	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	2006	All	x86_64	All

Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	2006	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux</a>	2006	All	x86_64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linuxsoft 2007</a>	All	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linuxsoft 2007</a>	All	All	x86_64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linuxsoft 2007</a>	All	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linuxsoft 2007</a>	All	All	x86_64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	3.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	3.0	All	x86_64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	4.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	4.0	All	x86_64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	3.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	3.0	All	x86_64	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	4.0	All	All	All
Operating System	<a href="#">Mandrakesoft</a>	<a href="#">Mandrake Linux Corporate Server</a>	4.0	All	x86_64	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.10	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.11	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.12	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.13	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.14	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.14a	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.20	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.20a	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.20b	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.21	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.21a	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.21b	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.21c	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.22	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.23d	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.6	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.7	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.8	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.9	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.10	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.11	All	All	All

Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.12	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.13	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.14	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.14a	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.20	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.20a	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.20b	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.21	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.21a	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.21b	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.21c	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.22	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.23d	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.6	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.7	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.8	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.9	All	All	All

## References

Reference	Source
SecurityFocus	BUGTR
2007-0007	TRUSTI
Samba - Security Announcement Archive	CONFIF
Ubuntu update for samba - Advisories - Secunia	SECUN
Gentoo update for samba - Advisories - Secunia	SECUN
SecurityFocus	BUGTR
Mandriva update for samba - Advisories - Secunia	SECUN
Gentoo Linux Documentation -- Samba: Multiple vulnerabilities	GENTO
Samba Denial of Service and Format String Vulnerability - Advisories - Secunia	SECUN
OpenPKG Corporation: Security: Security Advisories	OPENP
The Slackware Linux Project: Slackware Security Advisories	SLACK
Slackware update for samba - Advisories - Secunia	SECUN
Trustix Update for Various Packages - Advisories - Secunia	SECUN
SecurityTracker.com Archives - Samba Format String Bug in 'afsacl.so' VFS Plugin May Let Remote Users Execute Arbitrary Code	SECTR
Debian update for samba - Advisories - Secunia	SECUN
Webmail - OVH	VUPEN

IBM X-Force Exchange	XF
Samba Server VFS Plugin AFSACL.SO Remote Format String Vulnerability	BID
Advisories   Mandriva	MANDR
Debian -- Security Information -- DSA-1257-1 samba	DEBIAN
33101	OSVDB
issues.rpath.com/browse/RPL-1005	CONFIF
USN-419-1: Samba vulnerabilities   Ubuntu	UBUNT
US-CERT Vulnerability Notes	CERT-V
CVE Program record	CVE.OF
NVD vulnerability detail	NVD

### Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2007-05-14	Mark J Cox	Not vulnerable. These issues affect the AFS ACL module which is not distributed with Samba in

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)