



# CVE-2007-2447

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

## Summary

<b>CVE</b>	CVE-2007-2447
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2007-05-14 21:19:00 UTC
<b>Updated</b>	2018-10-16 16:43:00 UTC
<b>Description</b>	The MS-RPC functionality in smbd in Samba 3.0.0 through 3.0.25rc3 allows remote attackers to execute arbitrary commands

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.0	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.1	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>	3.0.15	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.16	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.17	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.18	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.19	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.2	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>	3.0.23	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.23a	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.23b	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.23c	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>	3.0.24	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.25	pre1	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.25	pre2	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.25	rc1	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.25	rc2	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.25	rc3	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.2a	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.3	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.4	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.4	rc1	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.5	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>	3.0.0	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.1	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>	3.0.15	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.16	All	All	All

Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.17	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.18	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.19	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.2	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>	3.0.23	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.23a	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.23b	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.23c	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>	3.0.24	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.25	pre1	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.25	pre2	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.25	rc1	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.25	rc2	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.25	rc3	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.2a	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.3	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.4	All	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.4	rc1	All	All
Application	<a href="#">Samba</a>	<a href="#">Samba</a>	3.0.5	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

About Security Update 2007-007

SUSE update for samba - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Samba - Security Announcement Archive
rPath update for samba and samba-swat - Advisories - Secunia
SecurityTracker.com Archives - Samba 'smb.conf' Scripts Input Validation Flaw Lets Remote Users Inject Arbitrary Commands
SuSE Security announcements: [suse-security-announce] SUSE Security Announcement: samba security problems (SUSE-SA:2007:031)
Webmail - OVH
20070514 Samba SAMR Change Password Remote Command Injection Vulnerability
Red Hat update for samba - Advisories - Secunia
HP Internet Express for Tru64 UNIX Samba Vulnerabilities - Advisories - Secunia
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
<a href="http://www.xerox.com/downloads/usa/en/c/cert_XRX08_001.pdf">www.xerox.com/downloads/usa/en/c/cert_XRX08_001.pdf</a>
[Full-Disclosure] Mailing List Charter
Mandriva update for samba - Advisories - Secunia
Webmail - OVH
Repository / Oval Repository
APPLE-SA-2007-07-31 Security Update 2007-007
#200588: Multiple Security Vulnerabilities in samba(7) May Allow Remote Code Execution, Elevation of Privileges, Remote Shell Command E
SecurityFocus
The Slackware Linux Project: Slackware Security Advisories
2007-0017
Gentoo update for samba - Advisories - Secunia
VMware ESX Server Multiple Security Updates - Advisories - Secunia
Sun Solaris Multiple Samba Vulnerabilities - Advisories - Secunia
Gentoo update for vmware - Advisories - Secunia
OpenPKG Corporation: Security: Security Advisories
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
200588
Gentoo Linux Documentation -- Samba: Multiple vulnerabilities
USN-460-1: Samba vulnerabilities   Ubuntu
Security Announcement
Debian update for samba - Advisories - Secunia
Debian -- Security Information -- DSA-1291-1 samba
Xerox ESS/Network Controller Samba Vulnerabilities - Advisories - Secunia
HPSBUX02218 SSRT071424 rev.1 - HP-UX running CIFS Server (Samba), Remote Arbitrary Code Execution - c01067768 - HP Business Su
34700

issues.rpath.com/browse/RPL-1366

SecurityFocus

HP Support document - HP Support Center

Webmail - OVH

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Samba MS-RPC Remote Shell Command Execution Vulnerability

Ubuntu update for samba - Advisories - Secunia

Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia

Advisories - Mandriva Linux

US-CERT Vulnerability Notes

Samba Multiple Vulnerabilities - Advisories - Secunia

SUSE Update for Multiple Packages - Advisories - Secunia

rhn.redhat.com | Red Hat Support

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

Trustix Updates for Multiple Packages - Advisories - Secunia

Apple Mac OS X 2007-007 Multiple Security Vulnerabilities

Slackware update for samba - Advisories - Secunia

About Secunia Research | Flexera

Samba 3.0.0 - 3.0.25rc3: Remote Command Injection Vulnerability - CXSecurity.com

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

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](#).

**Free CVE JSON API** [cve.report/api](#)

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