CVE-2007-2447

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2007-2447
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-05-14 21:19:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The MS-RPC functionality in smbd in Samba 3.0.0 through 3.0.25rc3 allows remote attackers to execute arbitrary commanc

Risk And Classification

Primary CVSS: v2.0 6 from nvd@nist.gov

AV:N/AC:M/Au:S/C:P/I:P/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

Single

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:S/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Samba	Samba	3.0.0	All	All	All

Application	Samba	Samba	3.0.1	All	All	All
Application	Samba	Samba	3.0.10	All	All	All
Application	Samba	Samba	3.0.11	All	All	All
Application	Samba	Samba	3.0.12	All	All	All
Application	Samba	Samba	3.0.13	All	All	All
Application	Samba	Samba	3.0.14	All	All	All
Application	Samba	Samba	3.0.14a	All	All	All
Application	Samba	Samba	3.0.15	All	All	All
Application	Samba	Samba	3.0.16	All	All	All
Application	Samba	Samba	3.0.17	All	All	All
Application	Samba	Samba	3.0.18	All	All	All
Application	Samba	Samba	3.0.19	All	All	All
Application	Samba	Samba	3.0.2	All	All	All
Application	Samba	Samba	3.0.20	All	All	All
Application	Samba	Samba	3.0.20a	All	All	All
Application	Samba	Samba	3.0.20b	All	All	All
Application	Samba	Samba	3.0.21	All	All	All
Application	Samba	Samba	3.0.21a	All	All	All
Application	Samba	Samba	3.0.21b	All	All	All
Application	Samba	Samba	3.0.21c	All	All	All
Application	Samba	Samba	3.0.22	All	All	All
Application	Samba	Samba	3.0.23	All	All	All
Application	Samba	Samba	3.0.23a	All	All	All
Application	Samba	Samba	3.0.23b	All	All	All
Application	Samba	Samba	3.0.23c	All	All	All
Application	Samba	Samba	3.0.23d	All	All	All
Application	Samba	Samba	3.0.24	All	All	All
Application	Samba	Samba	3.0.25	pre1	All	All
Application	Samba	Samba	3.0.25	pre2	All	All
Application	Samba	Samba	3.0.25	rc1	All	All
Application	Samba	Samba	3.0.25	rc2	All	All
Application	Samba	Samba	3.0.25	rc3	All	All
Application	Samba	Samba	3.0.2a	All	All	All
Application	Samba	Samba	3.0.3	All	All	All
Application	Samba	Samba	3.0.4	All	All	All
Application	Samba	Samba	3.0.4	rc1	All	All

Application	Samba	Samba	3.0.5	All	All	All
Application	Samba	Samba	3.0.6	All	All	All
Application	Samba	Samba	3.0.7	All	All	All
Application	Samba	Samba	3.0.8	All	All	All
Application	Samba	Samba	3.0.9	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Red Hat update for samba - Advisories - Secunia
SUSE update for samba - Secunia Advisories - Vulnerability Intelligence - Secunia.com
APPLE-SA-2007-07-31 Security Update 2007-007
USN-460-1: Samba vulnerabilities | Ubuntu
www.openwall.com/lists/oss-security/2025/10/16/2
VMware ESX Server Multiple Security Updates - Advisories - Secunia
[Full-Disclosure] Mailing List Charter
US-CERT Vulnerability Notes
SuSE Security announcements: [suse-security-announce] SUSE Security Announcement: samba security problems (SUSE-SA:2007:031)
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
Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia
Debian -- Security Information -- DSA-1291-1 samba
Samba 3.0.0 - 3.0.25rc3: Remote Command Injection Vulnerability - CXSecurity.com
Debian update for samba - Advisories - Secunia
Apple Mac OS X 2007-007 Multiple Security Vulnerabilities
issues.rpath.com/browse/RPL-1366
Slackware update for samba - Advisories - Secunia
OpenPKG Corporation: Security: Security Advisories
www.xerox.com/downloads/usa/en/c/cert_XRX08_001.pdf
HP Internet Express for Tru64 UNIX Samba Vulnerabilities - Advisories - Secunia
Security Announcement
Gentoo update for vmware - Advisories - Secunia

About Security Update 2007-007
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Samba Multiple Vulnerabilities - Advisories - Secunia
Gentoo update for samba - Advisories - Secunia
Repository / Oval Repository
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Mandriva update for samba - Advisories - Secunia
The Slackware Linux Project: Slackware Security Advisories
sunsolve.sun.com/search/document.do
Gentoo Linux Documentation -- Samba: Multiple vulnerabilities
www.trustix.org/errata/2007/0017
Samba MS-RPC Remote Shell Command Execution Vulnerability
rhn.redhat.com | Red Hat Support
HP Support document - HP Support Center
Samba - Security Announcement Archive
Advisories - Mandriva Linux
Sun Solaris Multiple Samba Vulnerabilities - Advisories - Secunia
Webmail - OVH
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Webmail - OVH
#200588: Multiple Security Vulnerabilities in samba(7) May Allow Remote Code Execution, Elevation of Privileges, Remote Shell Command E
www.osvdb.org/34700
Ubuntu update for samba - Advisories - Secunia
Webmail - OVH
HPSBUX02218 SSRT071424 rev.1 - HP-UX running CIFS Server (Samba), Remote Arbitrary Code Execution - c01067768 - HP Business Su
labs.idefense.com/intelligence/vulnerabilities/display.php
Xerox ESS/Network Controller Samba Vulnerabilities - Advisories - Secunia
SecurityFocus
SUSE Update for Multiple Packages - Advisories - Secunia
About Secunia Research | Flexera
SecurityFocus
Trustix Updates for Multiple Packages - Advisories - Secunia
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 registred 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**