



CVE-2007-4572

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

Summary

CVE	CVE-2007-4572
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-11-16 18:46:00 UTC
Updated	2018-10-30 16:25:00 UTC
Description	Stack-based buffer overflow in nmbd in Samba 3.0.0 through 3.0.26a, when configured as a Primary or Backup Domain controller.

Risk And Classification

Problem Types: CWE-119

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

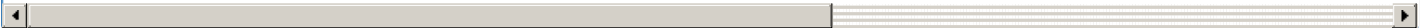
Application	Samba	Samba	3.0.21	All	All	All
Application	Samba	Samba	3.0.21a	All	All	All
Application	Samba	Samba	3.0.21b	All	All	All
Application	Samba	Samba	3.0.21c	All	All	All
Application	Samba	Samba	3.0.22	All	All	All
Application	Samba	Samba	3.0.23	All	All	All
Application	Samba	Samba	3.0.23a	All	All	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	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	3.0.25a	All	All	All
Application	Samba	Samba	3.0.25b	All	All	All
Application	Samba	Samba	3.0.25c	All	All	All
Application	Samba	Samba	3.0.26	All	All	All
Application	Samba	Samba	3.0.26a	All	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
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	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	3.0.25a	All	All	All
Application	Samba	Samba	3.0.25b	All	All	All
Application	Samba	Samba	3.0.25c	All	All	All
Application	Samba	Samba	3.0.26	All	All	All
Application	Samba	Samba	3.0.26a	All	All	All
Application	Samba	Samba	3.0.26b	All	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

References
Reference
HPSBUX02341
Apple Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia
Samba NMBD Logon Request Remote Buffer Overflow Vulnerability
issues.rpath.com/browse/RPL-1894
Repository / Oval Repository
US-CERT Technical Cyber Security Alert TA07-352A -- Apple Updates for Multiple Vulnerabilities
Solaris Samba Multiple Vulnerabilities - Advisories - Secunia
The Slackware Linux Project: Slackware Security Advisories
VMSA-2008-0001.1 - VMware
VMware ESX Server Multiple Security Updates - Advisories - Secunia
SecurityFocus
Samba Multiple Buffer Overflow Vulnerabilities - Advisories - Secunia
HP-UX HP CIFS Server Multiple Vulnerabilities - Advisories - Secunia
SecurityTracker.com Archives - Samba nmbd Buffer Overflow in Processing GETDC mailslot Requests Lets Remote Users Execute Arbitrary
About Security Update 2007-009
[Security-announce] VMSA-2008-0001 Moderate OpenPegasus PAM Authentication Buffer Overflow and updated service console packages
237764
rhn.redhat.com Red Hat Support
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
APPLE-SA-2007-12-17 Security Update 2007-009
Gentoo Linux Documentation -- Samba: Execution of arbitrary code
USN-544-2: Samba regression Ubuntu
HP-UX HP CIFS Server Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Slackware update for samba - Advisories - Secunia

Debian update for samba - Advisories - Secunia
rhnl.redhat.com Red Hat Support
SUSE update for samba - Advisories - Secunia
rPath update for samba - Advisories - Secunia
Webmail- OVH
Advisories Mandriva
Debian -- Security Information -- DSA-1409-3 samba
Ubuntu update for samba - Secunia Advisories - Vulnerability Intelligence - Secunia.com
Repository / Oval Repository
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
HPSBUX02316
rhnl.redhat.com Red Hat Support
Ubuntu update for samba - Advisories - Secunia
Mandriva update for samba - Advisories - Secunia
Webmail - OVH
Samba - Security Announcement Archive
Security Announcement
Fedora update for samba - Advisories - Secunia
SecurityFocus
[SECURITY] Fedora 7 Update: samba-3.0.27-0.fc7
Webmail - OVH
USN-544-1: Samba vulnerabilities Ubuntu security notices
Webmail - OVH
IBM X-Force Exchange
Red Hat update for samba - Advisories - Secunia
USN-617-1: Samba vulnerabilities Ubuntu
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.

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