



CVE-2006-3403

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

Summary

CVE	CVE-2006-3403
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-07-12 19:05:00 UTC
Updated	2018-10-18 16:47:00 UTC
Description	The smdb daemon (smbd/service.c) in Samba 3.0.1 through 3.0.22 allows remote attackers to cause a denial of service (m

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	3.0.20a	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	3.0.3	All	All	All
Application	Samba	Samba	3.0.4	All	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	3.0.1	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	3.0.20a	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	3.0.3	All	All	All
Application	Samba	Samba	3.0.4	All	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						Source
SecurityFocus						BUGTRAQ
Mac OS X Security Update Fixes Multiple Vulnerabilities - Advisories - Secunia						SECUNIA
SecurityFocus						HP
Advisories - Mandriva Linux						MANDRIVA
SecurityFocus						BUGTRAQ
US-CERT Technical Cyber Security Alert TA06-333A -- Apple Releases Security Update to Address Multiple Vulnerabilities						CERT
Debian update for samba - Advisories - Secunia						SECUNIA
VMware ESX Server 2.0.2 Upgrade Patch 2 (for 2.0.2 Systems)						CONFIRM
usn/usn-314-1 - Ubuntu: Linux for human beings						UBUNTU
Secunia - Advisories - Mandriva update for samba						SECUNIA
Trustix updates for gnupg/samba - Advisories - Secunia						SECUNIA
Security Announcement						SUSE
SecurityFocus						BUGTRAQ
SecurityTracker.com Archives - Samba smbd Memory Limit Error in make_connection() Lets Remote Users Deny Service						SECTrack
VMware ESX Server Multiple Vulnerabilities - Advisories - Secunia						SECUNIA
APPLE-SA-2006-11-28 Security Update 2006-007						APPLE
VMware ESX Server 2.1.3 Upgrade Patch 2 (for 2.1.3 Systems Only)						CONFIRM
SecurityFocus						BUGTRAQ
SecurityFocus						BUGTRAQ
Repository / Oval Repository						OVAL
Support						REDHAT
Samba - Security Announcement Archive						CONFIRM
Samba Internal Data Structures Denial of Service Vulnerability						BID
SecurityFocus						BUGTRAQ
Samba Multiple Share Connection Requests Denial of Service - Advisories - Secunia						SECUNIA
IBM X-Force Exchange						XF
The Slackware Linux Project: Slackware Security Advisories						SLACKWARE
exploits , vulnerabilities , articles , Samba Internal Data Structures DOS Vulnerability Exploit						MISC
SGI Advanced Linux Environment Multiple Updates - Advisories - Secunia						SECUNIA
Secunia - Advisories - Ubuntu update for samba						SECUNIA
Webmail - OVH						VUPEN

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
20060703-01-P	SGI
SecurityFocus	BUGTRAQ
About the security content of Security Update 2006-007	CONFIRM
SecurityFocus	BUGTRAQ
Gentoo update for samba - Advisories - Secunia	SECUNIA
Debian -- Security Information -- DSA-1110-1 samba	DEBIAN
VU#313836 - Samba fails to properly handle multiple share connection requests	CERT-VN
Secunia - Advisories - rPath update for samba	SECUNIA
SUSE Updates for Multiple Packages - Advisories - Secunia	SECUNIA
Slackware update for samba - Secunia.com	SECUNIA
Secunia - Advisories - Red Hat update for samba	SECUNIA
Gentoo Linux Documentation -- Samba: Denial of Service vulnerability	GENTOO
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD



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](#)