



CVE-2008-4314

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

Summary

CVE	CVE-2008-4314
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-12-01 15:30:00 UTC
Updated	2011-03-08 03:12:00 UTC
Description	smbd in Samba 3.0.29 through 3.2.4 might allow remote attackers to read arbitrary memory and cause a denial of service v

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Samba	Samba	3.0.29	All	All	All
Application	Samba	Samba	3.0.30	All	All	All
Application	Samba	Samba	3.0.31	All	All	All
Application	Samba	Samba	3.0.32	All	All	All
Application	Samba	Samba	3.0.33	All	All	All
Application	Samba	Samba	3.2.0	All	All	All
Application	Samba	Samba	3.2.1	All	All	All
Application	Samba	Samba	3.2.2	All	All	All
Application	Samba	Samba	3.2.3	All	All	All
Application	Samba	Samba	3.2.4	All	All	All
Application	Samba	Samba	3.0.29	All	All	All
Application	Samba	Samba	3.0.30	All	All	All
Application	Samba	Samba	3.0.31	All	All	All
Application	Samba	Samba	3.0.32	All	All	All
Application	Samba	Samba	3.0.33	All	All	All
Application	Samba	Samba	3.2.0	All	All	All
Application	Samba	Samba	3.2.1	All	All	All

Application	Samba	Samba	3.2.2	All	All	All
Application	Samba	Samba	3.2.3	All	All	All
Application	Samba	Samba	3.2.4	All	All	All

References						
Reference						Source
Webmail - OVH						VUPEN
Slackware update for samba - Secunia Advisories - Vulnerability Intelligence - Secunia.com						SECUNIA
Ubuntu update for samba - Secunia.com						SECUNIA
'[security bulletin] HPSBTU02454 SSRT080172 rev.1 - HP Internet Express for Tru64 UNIX Running Samba,' - MARC						HP
[SECURITY] Fedora 8 Update: samba-3.0.33-0.fc8						FEDORA
us1.samba.org/samba/ftp/patches/security/samba-3.0.32-CVE-2008-4314.patch						CONFIRM
[security-announce] SUSE Security Summary Report: SUSE-SR:2008:027						SUSE
Samba Arbitrary Memory Contents Information Disclosure Vulnerability						BID
Fedora update for samba - Secunia Advisories - Vulnerability Intelligence - Secunia.com						SECUNIA
Samba - Security Announcement Archive						CONFIRM
249087						SUNALE
The Slackware Linux Project: Slackware Security Advisories						SLACKW
[SECURITY] Fedora 9 Update: samba-3.2.5-0.22.fc9						FEDORA
HP Internet Express for Tru64 UNIX Samba Information Disclosure - Secunia Advisories - Vulnerability Information - Secunia.com						SECUNIA
50230						OSVDB
Webmail - OVH						VUPEN
Samba "smbd" Information Disclosure Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com						SECUNIA
USN-680-1: Samba vulnerability Ubuntu						UBUNTU
Webmail - OVH						VUPEN
SecurityTracker.com Archives - Samba 'trans', 'trans2', and 'nttrans' Requests Let Remote Users Obtain Memory Contents						SECTRA
CVE Program record						CVE.ORG
NVD vulnerability detail						NVD

Vendor Comments And Credit			
Organization	Published	Contributor	Statement
Red Hat	2008-12-01	Joshua Bressers	Not vulnerable. This issue did not affect the versions of Samba as shipped with Red Hat Enterprise Linux 4.

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](#)