



CVE-2009-1886

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

Summary

CVE	CVE-2009-1886
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-06-25 01:30:00 UTC
Updated	2017-08-17 01:30:00 UTC
Description	Multiple format string vulnerabilities in client/client.c in smbclient in Samba 3.2.0 through 3.2.12 might allow context-depend

Risk And Classification

Problem Types: CWE-134

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Samba	Samba	3.2.0	All	All	All
Application	Samba	Samba	3.2.1	All	All	All
Application	Samba	Samba	3.2.10	All	All	All
Application	Samba	Samba	3.2.11	All	All	All
Application	Samba	Samba	3.2.12	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	3.2.5	All	All	All
Application	Samba	Samba	3.2.6	All	All	All
Application	Samba	Samba	3.2.7	All	All	All
Application	Samba	Samba	3.2.8	All	All	All
Application	Samba	Samba	3.2.9	All	All	All
Application	Samba	Samba	3.2.0	All	All	All
Application	Samba	Samba	3.2.1	All	All	All
Application	Samba	Samba	3.2.10	All	All	All
Application	Samba	Samba	3.2.11	All	All	All

Application	Samba	Samba	3.2.12	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	3.2.5	All	All	All
Application	Samba	Samba	3.2.6	All	All	All
Application	Samba	Samba	3.2.7	All	All	All
Application	Samba	Samba	3.2.8	All	All	All
Application	Samba	Samba	3.2.9	All	All	All

References						
Reference					Source	Li
www.samba.org/samba/ftp/patches/security/samba-3.2.12-CVE-2009-1886.patch					CONFIRM	w
Samba Security Bypass and Format String Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com					SECUNIA	se
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH					VUPEN	w
Ubuntu update for samba - Secunia Advisories - Vulnerability Information - Secunia.com					SECUNIA	se
Support / Security / Advisories / / MDVSA-2009:196 Mandriva					MANDRIVA	w
Slackware update for samba - Secunia.com					SECUNIA	se
SecurityTracker.com Archives - Samba smbclient Format String Bug May Let Users Execute Arbitrary Code					SECTRACK	w
USN-839-1: Samba vulnerabilities Ubuntu					UBUNTU	w
6478 – smbclient interpolates % character in remote file name; CVE-2009-1886					CONFIRM	bu
Samba - Security Announcement Archive					CONFIRM	w
IBM X-Force Exchange					XF	e>
Debian update for samba - Secunia.com					SECUNIA	se
The Slackware Linux Project: Slackware Security Advisories					SLACKWARE	w
Samba Format String And Security Bypass Vulnerabilities					BID	w
Debian -- Security Information -- DSA-1823-1 samba					DEBIAN	w
CVE Program record					CVE.ORG	w
NVD vulnerability detail					NVD	nv

Vendor Comments And Credit			
Organization	Published	Contributor	Statement
Red Hat	2009-06-29	Tomas Hoger	Not vulnerable. This issue did not affect the versions of samba as shipped with Red Hat Enterp

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](#)