



CVE-2017-9461

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

Summary

CVE	CVE-2017-9461
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-06 21:29:00 UTC
Updated	2023-11-07 02:50:00 UTC
Description	smbd in Samba before 4.4.10 and 4.5.x before 4.5.6 has a denial of service vulnerability (fd_open_atomic infinite loop with

Risk And Classification

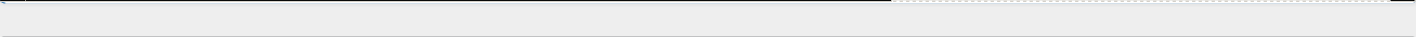
Problem Types: CWE-835

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All

Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Samba	Samba	4.5.0	All	All	All
Application	Samba	Samba	4.5.1	All	All	All
Application	Samba	Samba	4.5.2	All	All	All
Application	Samba	Samba	4.5.3	All	All	All
Application	Samba	Samba	4.5.4	All	All	All
Application	Samba	Samba	4.5.5	All	All	All
Application	Samba	Samba	4.5.0	All	All	All
Application	Samba	Samba	4.5.1	All	All	All
Application	Samba	Samba	4.5.2	All	All	All
Application	Samba	Samba	4.5.3	All	All	All
Application	Samba	Samba	4.5.4	All	All	All
Application	Samba	Samba	4.5.5	All	All	All
Application	Samba	Samba	All	All	All	All

References						
Reference				Source	Link	
Red Hat Customer Portal				REDHAT	access.redhat.com	
#864291 - samba: CVE-2017-9461: infinite loop on bad-symlink resolution - Debian Bug report logs				CONFIRM	bugs.debian.org	
git.samba.org - samba.git/commit				CONFIRM	git.samba.org	
Samba CVE-2017-9461 Remote Denial of Service Vulnerability				BID	www.securityfocus.	
Red Hat Customer Portal				REDHAT	access.redhat.com	
git.samba.org - samba.git/commit					git.samba.org	
[SECURITY] [DLA 1754-1] samba security update				MLIST	lists.debian.org	
Red Hat Customer Portal				REDHAT	access.redhat.com	
Bug 12572 – fd_open_atomic() can loop indefinitely when trying to open an invalid symlink with O_CREAT				CONFIRM	bugzilla.samba.org	
CVE Program record				CVE.ORG	www.cve.org	
NVD vulnerability detail				NVD	nvd.nist.gov	



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](#)