



CVE-2017-8849

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

Summary

CVE	CVE-2017-8849
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-17 14:29:00 UTC
Updated	2019-03-18 16:41:00 UTC
Description	smb4k before 2.0.1 allows local users to gain root privileges by leveraging failure to verify arguments to the mount helper D

Risk And Classification

Problem Types: CWE-20

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
Application	Smb4k Project	Smb4k	All	All	All	All

References

Reference	Source	Link
smb4k.git - The advanced network neighborhood browser and Samba share mounting utility by KDE.	CONFIRM	cgit.kde.org
Bug 1449656 – CVE-2017-8849 smb4k: unauthorized local command execution as root	CONFIRM	bugzilla.redhat.com
oss-security - generic kde LPE	MLIST	www.openwall.com
Debian -- Security Information -- DSA-3951-1 smb4k	DEBIAN	www.debian.org
KDE 4/5 - 'KAuth' Local Privilege Escalation - Linux local Exploit	EXPLOIT-DB	www.exploit-db.com
Smb4K: Arbitrary command execution as root (GLSA 201705-14) — Gentoo security	GENTOO	security.gentoo.org
smb4k.git - The advanced network neighborhood browser and Samba share mounting utility by KDE.	CONFIRM	cgit.kde.org
www.kde.org/info/security/advisory-20170510-2.txt	CONFIRM	www.kde.org
Juju CVE-2017-8849 Local Privilege Escalation Vulnerability	BID	www.securityfocus.co
Smb4K CVE-2017-8849 Local Privilege Escalation Vulnerability	BID	www.securityfocus.co
CVE Program record	CVE.ORG	www.cve.org

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[710367](#) Gentoo Linux Smb4K Arbitrary command execution as root Vulnerability (GLSA 201705-14)

© [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