



CVE-2018-7169

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2018-7169
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-15 20:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	An issue was discovered in shadow 4.5. newgidmap (in shadow-utils) is setuid and allows an unprivileged user to be placed

Risk And Classification

Problem Types: CWE-732

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Shadow Project	Shadow	4.5	All	All	All
Application	Shadow Project	Shadow	4.5	All	All	All

References

Reference	Source	Link	Ta
Shadow: security bypass (GLSA 201805-09) — Gentoo Security	GENTOO	security.gentoo.org	TI
Bug #1729357 "unprivileged user can drop supplementary groups" : Bugs : shadow package : Ubuntu	MISC	bugs.launchpad.net	E:
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[198646](#) Ubuntu Security Notification for shadow Vulnerabilities (USN-5254-1)

[710271](#) Gentoo Linux Shadow security bypass Vulnerability (GLSA 201805-09)

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)