CVE-2016-7097

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2016-7097
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-10-16 21:59:11 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The filesystem implementation in the Linux kernel through 4.8.2 preserves the setgid bit during a setxattr call, which allows

Risk And Classification

Primary CVSS: v3.0 4.4 MEDIUM from nvd@nist.gov

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

EPSS: 0.000530000 probability, percentile 0.164060000 (date 2026-05-07)

Problem Types: CWE-285 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	4.4	MEDIUM	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N
2.0	nvd@nist.gov	Primary	3.6		AV:L/AC:L/Au:N/C:P/I:P/A:N

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

None

AV:L/AC:L/Au:N/C:P/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
Red Hat Customer Portal
support.f5.com/csp/article/K31603170
USN-3146-2: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu
'[PATCH v2] posix_acl: Clear SGID bit when setting file permissions' - MARC
Android Security Bulletin—April 2017 | Android Open Source Project
[PATCH 2/2] posix_acl: Clear SGID bit when modifying file permissions — Linux Filesystem Development
posix_acl: Clear SGID bit when setting file permissions · torvalds/linux@0739310 · GitHub
USN-3146-1: Linux kernel vulnerabilities | Ubuntu
Google Android Multiple Flaws Let Users Deny Service, Obtain Potentially Sensitive Information, and Gain Elevated Privileges and Let Remot

Google Android Multiple Flaws Let Users Deny Service, Obtain Potentially Sensitive Information, and Gain Elevated Privileges and Let Remot
Red Hat Customer Portal
oss-security - Re: CVE request -- linux kernel: Setting a POSIX ACL via setxattr doesn't clear the setgid bit
USN-3147-1: Linux kernel vulnerabilities | Ubuntu
Linux Kernel Local Security Bypass Vulnerability
kernel/git/torvalds/linux.git - Linux kernel source tree
Red Hat Customer Portal
Bug 1368938 – CVE-2016-7097 kernel: Setting a POSIX ACL via setxattr doesn't clear the setgid bit
Red Hat Customer Portal
CONFIRM:https://support.f5.com/csp/article/K31603170?utm_source=f5support&utm_medium=RSS
Red Hat Customer Portal
CVE-2016-7097 - Red Hat Customer Portal
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**