



CVE-2016-6516

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

Summary

CVE	CVE-2016-6516
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-08-06 20:59:15 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Race condition in the ioctl_file_dedupe_range function in fs/ioctl.c in the Linux kernel through 4.7 allows local users to caus

Risk And Classification

Primary CVSS: v3.0 7.4 HIGH from nvd@nist.gov

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

Problem Types: CWE-119 | CWE-362 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	7.4	HIGH	CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	4.4		AV:L/AC:M/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

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	Source	Link
vfs: ioctl: prevent double-fetch in dedupe ioctl · torvalds/linux@10eec60 · GitHub	af854a3a-2127-422b-91ae-364da2661108	github.
Linux Kernel CVE-2016-6516 Local Heap Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.s
Bug 1362457 – CVE-2016-6516 kernel: vfs: ioctl: double fetch leading to heap overflow	af854a3a-2127-422b-91ae-364da2661108	bugzilla
kernel/git/torvalds/linux.git - Linux kernel source tree	af854a3a-2127-422b-91ae-364da2661108	git.ker
oss-security - CVE Request: Linux >= 4.5 double fetch leading to heap overflow	af854a3a-2127-422b-91ae-364da2661108	www.c
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

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](#)