CVE-2014-4014

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

Summary

CVE	CVE-2014-4014
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-06-23 11:21:17 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The capabilities implementation in the Linux kernel before 3.14.8 does not properly consider that namespaces are inapplica

Risk And Classification

Primary CVSS: v2.0 6.2 from nvd@nist.gov

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

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

High

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

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
Bug 1107966 – CVE-2014-4014 Kernel: possible privilege escalation in user namespace	af854a3a-2127-422b-9
kernel/git/torvalds/linux.git - Linux kernel source tree	af854a3a-2127-422b-9
Linux Kernel inode_capable() Incorrect Capability Check Lets Local Users Gain Elevated Privileges - SecurityTracker	af854a3a-2127-422b-9
Linux Kernel CVE-2014-4014 Local Privilege Escalation Vulnerability	af854a3a-2127-422b-9
Linux Kernel <= 3.13 - Local Privilege Escalation PoC (gid)	af854a3a-2127-422b-9
Android Security Bulletin—December 2016 | Android Open Source Project	af854a3a-2127-422b-9
fs,userns: Change inode_capable to capable_wrt_inode_uidgid · torvalds/linux@23adbe1 · GitHub	af854a3a-2127-422b-9
oss-security - CVE-2014-4014: Linux kernel user namespace bug	af854a3a-2127-422b-9
About Secunia Research | Flexera	af854a3a-2127-422b-9
www.kernel.org/pub/linux/kernel/v3.x/ChangeLog-3.14.8	af854a3a-2127-422b-9
kernel/git/torvalds/linux.git - Linux kernel source tree	MITRE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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