CVE-2014-2851

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

Summary

CVE	CVE-2014-2851
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-04-14 23:55:07 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Integer overflow in the ping_init_sock function in net/ipv4/ping.c in the Linux kernel through 3.14.1 allows local users to caus

Risk And Classification

Primary CVSS: v2.0 6.9 from nvd@nist.gov

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

Problem Types: CWE-416 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:L/AC:M/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
Debian -- Security Information -- DSA-2926-1 linux	af854a3a-2127-422b-91ae-364da26611
LKML: "Wang, Xiaoming": [PATCH] net: ipv4: current group_info should be put after using.	af854a3a-2127-422b-91ae-364da26611
oss-security - Re: CVE request -- Linux kernel: net: ping: refcount issue in ping_init_sock() function	af854a3a-2127-422b-91ae-364da26611
Linux Kernel 'ping_init_sock()' Local Privilege Escalation Vulnerability	af854a3a-2127-422b-91ae-364da26611
Security Advisory SA59599 - Ubuntu update for kernel - Secunia	af854a3a-2127-422b-91ae-364da26611
Linux Kernel ping_init_sock() Counter Overflow Lets Local Users Deny Service - SecurityTracker	af854a3a-2127-422b-91ae-364da26611
Bug 1086730 – CVE-2014-2851 kernel: net: ping: refcount issue in ping_init_sock() function	af854a3a-2127-422b-91ae-364da26611
About Secunia Research | Flexera	af854a3a-2127-422b-91ae-364da26611
kernel/git/netdev/net.git - Netdev Group's networking tree	af854a3a-2127-422b-91ae-364da26611
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.