CVE-2015-8970

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

Summary

CVE	CVE-2015-8970
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-11-28 03:59:02 UTC
Updated	2026-05-06 22:30:45 UTC
Description	crypto/algif_skcipher.c in the Linux kernel before 4.4.2 does not verify that a setkey operation has been performed on an AF

Risk And Classification

Primary CVSS: v3.0 5.5 MEDIUM from nvd@nist.gov

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

EPSS: 0.000380000 probability, percentile 0.114680000 (date 2026-05-10)

Problem Types: CWE-476 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	5.5	MEDIUM	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
2.0	nvd@nist.gov	Primary	4.9		AV:L/AC:L/Au:N/C:N/I:N/A:C

CVSS v3.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

None

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

AV:L/AC:L/Au:N/C:N/I:N/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	Li
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661108	ac
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661108	ac
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661108	ac
oss-security - Re: CVE request -- linux kernel: crypto: GPF in lrw_crypt caused by null-deref	af854a3a-2127-422b-91ae-364da2661108	w
kernel/git/torvalds/linux.git - Linux kernel source tree	af854a3a-2127-422b-91ae-364da2661108	gi
crypto: algif_skcipher - Require setkey before accept(2) · torvalds/linux@dd50458 · GitHub	af854a3a-2127-422b-91ae-364da2661108	gi
Bug 1386286 – CVE-2015-8970 kernel: crypto: GPF in lrw_crypt caused by null-deref	af854a3a-2127-422b-91ae-364da2661108	bu
Linux Kernel 'crypto/lrw.c' Local Denial of Service Vulnerability	af854a3a-2127-422b-91ae-364da2661108	w
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.4.2	af854a3a-2127-422b-91ae-364da2661108	w

Google Grupper	af854a3a-2127-422b-91ae-364da2661108	g
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661108	a
Google Grupper	MITRE	g
CVE-2015-8970 - Red Hat Customer Portal	MITRE	a
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

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