CVE-2017-16939

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

Summary

CVE	CVE-2017-16939
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-11-24 10:29:00 UTC
Updated	2023-01-19 15:46:00 UTC
Description	The XFRM dump policy implementation in net/xfrm/xfrm_user.c in the Linux kernel before 4.13.11 allows local users to gain

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All
Operating System	Linux	Linux Kernel	All	All	All	All

References

Reference	Source	Link
Debian -- Security Information -- DSA-4082-1 linux	DEBIAN	www.debian.org
Red Hat Customer Portal	REDHAT	access.redhat.com
Bug 1069702 – VUL-0: CVE-2017-16939: kernel-source: local privilege escalation with XFRM sockets	MISC	bugzilla.suse.com
Full Disclosure: SSD Advisory – Linux Kernel XFRM Privilege Escalation	MISC	seclists.org
[SECURITY] [DLA 1200-1] linux security update	MLIST	lists.debian.org
Linux Kernel CVE-2017-16939 Local Privilege Escalation Vulnerability	BID	www.securityfocus.com
401 Authorization Required	MISC	blogs.securiteam.com
ipsec: Fix aborted xfrm policy dump crash · torvalds/linux@1137b5e · GitHub	MISC	github.com
Red Hat Customer Portal	REDHAT	access.redhat.com
Red Hat Customer Portal	REDHAT	access.redhat.com
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org

[security-announce] SUSE-SU-2018:0011-1: important: Security update for	SUSE	lists.opensuse.org
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.13.11	MISC	www.kernel.org
Red Hat Customer Portal	REDHAT	access.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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