CVE-2016-10153

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

Summary

CVE	CVE-2016-10153
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-06 06:59:00 UTC
Updated	2017-02-09 14:57:00 UTC
Description	The crypto scatterlist API in the Linux kernel 4.9.x before 4.9.6 interacts incorrectly with the CONFIG_VMAP_STACK optior

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux Kernel	4.9	All	All	All
Operating System	Linux	Linux Kernel	4.9.1	All	All	All
Operating System	Linux	Linux Kernel	4.9.2	All	All	All
Operating System	Linux	Linux Kernel	4.9.3	All	All	All
Operating System	Linux	Linux Kernel	4.9.4	All	All	All
Operating System	Linux	Linux Kernel	4.9.5	All	All	All
Operating System	Linux	Linux Kernel	4.9	All	All	All
Operating System	Linux	Linux Kernel	4.9.1	All	All	All
Operating System	Linux	Linux Kernel	4.9.2	All	All	All
Operating System	Linux	Linux Kernel	4.9.3	All	All	All
Operating System	Linux	Linux Kernel	4.9.4	All	All	All
Operating System	Linux	Linux Kernel	4.9.5	All	All	All

References

Reference	Source	Link	Tags
libceph: introduce ceph_crypt() for in-place en/decryption · torvalds/linux@a45f795 · GitHub	CONFIRM	github.com	Issue Tr
www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.9.6	CONFIRM	www.kernel.org	Release

oss-security - Re: CVE REQUEST: linux kernel: process with pgid zero able to crash kernel	MLIST	www.openwall.com	Mailing l
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM	git.kernel.org	Issue Tr
Linux Kernel CVE-2016-10153 Local Denial of Service Vulnerability	BID	www.securityfocus.com	Third Pa
Bug 1416101 – CVE-2016-10153 kernel: introduce ceph_crypt() for in-place en/decryption	CONFIRM	bugzilla.redhat.com	Issue Tr
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**