CVE-2017-7889

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

Summary

CVE	CVE-2017-7889
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-17 00:59:00 UTC
Updated	2023-02-14 21:12:00 UTC
Description	The mm subsystem in the Linux kernel through 3.2 does not properly enforce the CONFIG_STRICT_DEVMEM protection n

Risk And Classification

Problem Types: CWE-732

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
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	Tags
Red Hat Customer Portal	REDHAT	access.redhat.com	
mm: Tighten x86 /dev/mem with zeroing reads · torvalds/linux@a4866aa · GitHub	MISC	github.com	Issue Trac
kernel/git/tip/tip.git - Unnamed repository; edit this file 'description' to name the repository.	CONFIRM	git.kernel.org	
Red Hat Customer Portal	REDHAT	access.redhat.com	
Red Hat Customer Portal	REDHAT	access.redhat.com	
Debian -- Security Information -- DSA-3945-1 linux	DEBIAN	www.debian.org	
USN-3583-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org	Issue Trac
USN-3583-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com	

oss-security - Silently (or obliviously) partially-fixed CONFIG_STRICT_DEVMEM bypass	MISC	www.openwall.com	Mailing Lis
Linux Kernel CVE-2017-7889 Multiple Local Security Bypass Vulnerabilities	BID	www.securityfocus.com	Third Part
Red Hat Customer Portal	REDHAT	access.redhat.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

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**