CVE-2018-18281

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

Summary

CVE	CVE-2018-18281
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-10-30 18:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	Since Linux kernel version 3.2, the mremap() syscall performs TLB flushes after dropping pagetable locks. If a syscall such

Risk And Classification

Problem Types: CWE-459

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	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.10	All	All	All
Operating System	Debian	Debian Linux	8.0	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

USN-3871-3: Linux kernel (AWS, GCP, KVM, OEM, Raspberry Pi 2) vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU
1695 - Linux: mremap() TLB flush too late with concurrent ftruncate() - project-zero - Monorail	MISC
Red Hat Customer Portal	REDHAT
USN-3832-1: Linux kernel (AWS) vulnerabilities | Ubuntu security notices	UBUNTU
cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.9.135	CONFIRM
USN-3835-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU
[SECURITY] [DLA 1715-1] linux-4.9 security update	MLIST
cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.18.16	CONFIRM
Red Hat Customer Portal	REDHAT
[SECURITY] [DLA 1731-2] linux regression update	MLIST
USN-3880-1: Linux kernel vulnerabilities | Ubuntu security notices | Ubuntu	UBUNTU
kernel/git/torvalds/linux.git - Linux kernel source tree	CONFIRM
USN-3871-5: Linux kernel (Azure) vulnerabilities | Ubuntu security notices	UBUNTU
USN-3880-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu security notices	UBUNTU
USN-3871-4: Linux kernel (HWE) vulnerabilities | Ubuntu security notices	UBUNTU
Red Hat Customer Portal	REDHAT
Linux Kernel CVE-2018-18281 Local Security Bypass Vulnerability	BID
Linux mremap() TLB Flush Too Late ≈ Packet Storm	MISC
oss-security - Linux kernel: TLB flush happens too late on mremap (CVE-2018-18281; fixed in 4.9.135, 4.14.78, 4.18.16, 4.19)	MLIST
[SECURITY] [DLA 1731-1] linux security update	MLIST
Linux Kernel Components Multiple Security Vulnerabilities	BID
Red Hat Customer Portal	REDHAT
USN-3871-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU
cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.14.78	CONFIRM
Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	REDHAT
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

376774 F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Linux kernel Vulnerability cve-2018-18281 (K36462841)

Free CVE JSON API cve.report/api

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