CVE-2019-9213

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2019-9213
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-05 22:29:00 UTC
Updated	2022-10-12 15:56:00 UTC
Description	In the Linux kernel before 4.20.14, expand_downwards in mm/mmap.c lacks a check for the mmap minimum address, whic

Risk And Classification

Problem Types: CWE-476

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	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	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	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

Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Opensuse	Leap	15.0	All	All	All
Operating System	Opensuse	Leap	42.3	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All

References

Reference	Source	Link
cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.19.27	MISC	cdn.kernel.org
cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.14.105	MISC	cdn.kernel.org
Linux < 4.20.14 - Virtual Address 0 is Mappable via Privileged write() to /proc/*/mem - Linux dos Exploit	EXPLOIT-DB	www.exploit-db.com
USN-3932-2: Linux kernel (Xenial HWE) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
mm: enforce min addr even if capable() in expand_downwards() · torvalds/linux@0a1d529 · GitHub	MISC	github.com
[SECURITY] [DLA 1731-2] linux regression update	MLIST	lists.debian.org
USN-3930-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
USN-3930-2: Linux kernel (HWE) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
Red Hat Customer Portal	REDHAT	access.redhat.com
Linux kernel CVE-2019-9213 Local Denial of Service Vulnerability	BID	www.securityfocus.c
[security-announce] openSUSE-SU-2019:1085-1: important: Security update	SUSE	lists.opensuse.org
[SECURITY] [DLA 1771-1] linux-4.9 security update	MLIST	lists.debian.org
USN-3932-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
USN-3933-2: Linux kernel (Trusty HWE) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
Reliable Datagram Sockets (RDS) rds_atomic_free_op Privilege Escalation ≈ Packet Storm	MISC	packetstormsecurity
USN-3931-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
[SECURITY] [DLA 1731-1] linux security update	MLIST	lists.debian.org
Red Hat Customer Portal	REDHAT	access.redhat.com
USN-3931-2: Linux kernel (HWE) vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
USN-3933-1: Linux kernel vulnerabilities | Ubuntu security notices	UBUNTU	usn.ubuntu.com
cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.9.162	MISC	cdn.kernel.org
[security-announce] openSUSE-SU-2019:1193-1: important: Security update	SUSE	lists.opensuse.org
cdn.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.20.14	MISC	cdn.kernel.org
kernel/git/torvalds/linux.git - Linux kernel source tree	MISC	git.kernel.org
1792 - project-zero - Project Zero - Monorail	MISC	bugs.chromium.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.

Legacy QID Mappings

160076 Oracle Enterprise Linux Security Update for unbreakable enterprise kernel (ELSA-2022-9761)

377042 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2019:0014)

390267 Oracle VM Server for x86 Security Update for kernel (OVMSA-2022-0024)