



# CVE-2019-9213

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

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

## 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	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.3	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.0	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	42.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All

## References

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

Hed Hat Customer Portal	HEDHAI	<a href="https://access.redhat.com">access.redhat.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

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)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)