



CVE-2020-25285

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

Summary

| | |
|------------------------|---|
| CVE | CVE-2020-25285 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2020-09-13 18:15:00 UTC |
| Updated | 2022-04-28 18:32:00 UTC |
| Description | A race condition between hugetlb sysctl handlers in mm/hugetlb.c in the Linux kernel before 5.8.8 could be used by local at |

Risk And Classification

Problem Types: [CWE-362](#) | [CWE-787](#) | [CWE-476](#)

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|---------------------------|------------------------------|---------|--------|---------|----------|
| 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 | 20.04 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |

References

| Reference |
|--|
| USN-4576-1: Linux kernel vulnerabilities Ubuntu security notices Ubuntu |
| [SECURITY] [DLA 2420-2] linux regression update |
| grsecurity on Twitter: "Bug fixed in today's 4.14 kernel was fixed in #grsecurity 6 years ago as part of CONSTIFY: https://t.co/sTLcs2qfyk..." |
| [SECURITY] [DLA 2385-1] linux-4.19 security update |
| cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.8.8 |
| CVE-2020-25285 Linux Kernel Vulnerability in NetApp Products NetApp Product Security |

[kernel/git/torvalds/linux.git](#) - Linux kernel source tree

[SECURITY] [DLA 2420-1] linux security update

[USN-4579-1: Linux kernel vulnerabilities](#) | [Ubuntu security notices](#) | [Ubuntu](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159185](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2021-1578)

[198328](#) Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-4912-1)

[239314](#) Red Hat Update for kernel-rt (RHSA-2021:1739)

[239339](#) Red Hat Update for kernel (RHSA-2021:1578)

[353100](#) Amazon Linux Security Advisory for kernel : ALAC2012-2021-024

[353101](#) Amazon Linux Security Advisory for kmod-mlx5 : ALAC2012-2021-025

[353102](#) Amazon Linux Security Advisory for kmod-sfc : ALAC2012-2021-026

[353135](#) Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-016

[377038](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2020:0198)

[610372](#) Google Pixel Android October 2021 Security Patch Missing

[6140131](#) AWS Bottlerocket Security Update for kernel (GHSA-3pwc-c3mh-xcv7)

[750376](#) OpenSUSE Security Update for RT kernel (openSUSE-SU-2021:0242-1)

[750533](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:2112-1)

[750609](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2020:1906-1)

[750738](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:3326-1)

[900076](#) CBL-Mariner Linux Security Update for kernel 5.4.91

[903239](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3456)

[905874](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3456-1)

[940354](#) AlmaLinux Security Update for kernel (ALSA-2021:1578)

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](#)