# CVE-2020-25671

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2020-25671 |
| **State** | PUBLIC |
| **Assigner** | secalert@redhat.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2021-05-26 11:15:00 UTC |
| **Updated** | 2023-02-12 23:40:00 UTC |
| **Description** | A vulnerability was found in Linux Kernel, where a refcount leak in llcp_sock_connect() causing use-after-free which might l |

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Fedoraproject | Fedora | 32 | All | All | All |
| Operating System | Fedoraproject | Fedora | 33 | All | All | All |
| Operating System | Fedoraproject | Fedora | 34 | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Application | Netapp | Active Iq Unified Manager | - | All | All | All |
| Application | Netapp | Cloud Backup | - | All | All | All |
| Hardware | Netapp | H300e | - | All | All | All |
| Operating System | Netapp | H300e Firmware | - | All | All | All |
| Hardware | Netapp | H300s | - | All | All | All |
| Operating System | Netapp | H300s Firmware | - | All | All | All |
| Hardware | Netapp | H410c | - | All | All | All |
| Operating System | Netapp | H410c Firmware | - | All | All | All |
| Hardware | Netapp | H410s | - | All | All | All |
| Operating System | Netapp | H410s Firmware | - | All | All | All |
| Hardware | Netapp | H500e | - | All | All | All |
| Operating System | Netapp | H500e Firmware | - | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Hardware | Netapp | H500s | - | All | All | All |
| Operating System | Netapp | H500s Firmware | - | All | All | All |
| Hardware | Netapp | H700e | - | All | All | All |
| Operating System | Netapp | H700e Firmware | - | All | All | All |
| Hardware | Netapp | H700s | - | All | All | All |
| Operating System | Netapp | H700s Firmware | - | All | All | All |
| Hardware | Netapp | Solidfire Baseboard Management Controller | - | All | All | All |
| Operating System | Netapp | Solidfire Baseboard Management Controller Firmware | - | All | All | All |

## References

| Reference | Source | L |
|---|---|---|
| oss-security - [CVE-2020-25670,CVE-2020-25671,CVE-2020-25672,CVE-2020-25673]Linux kernel: many bugs in nfc socket | MLIST | w |
| FEDORA-2021-d56567bdab | FEDORA | li |
| oss-security - [CVE-2020-25670,CVE-2020-25671,CVE-2020-25672,CVE-2020-25673]Linux kernel: many bugs in nfc socket | MISC | w |
| June 2021 Linux Kernel Vulnerabilities in NetApp Products \| NetApp Product Security | CONFIRM | s |
| [SECURITY] Fedora 33 Update: kernel-5.11.14-200.fc33 - package-announce - Fedora Mailing-Lists | FEDORA | li |
| [SECURITY] [DLA 2689-1] linux security update | MLIST | li |
| [SECURITY] Fedora 33 Update: kernel-5.11.14-200.fc33 - package-announce - Fedora Mailing-Lists | MISC | li |
| [SECURITY] Fedora 32 Update: kernel-tools-5.11.14-100.fc32 - package-announce - Fedora Mailing-Lists | FEDORA | li |
| [SECURITY] [DLA 2690-1] linux-4.19 security update | MLIST | li |
| [SECURITY] Fedora 34 Update: kernel-5.11.14-300.fc34 - package-announce - Fedora Mailing-Lists | MISC | li |
| [SECURITY] Fedora 32 Update: kernel-tools-5.11.14-100.fc32 - package-announce - Fedora Mailing-Lists | MISC | li |
| CVE Program record | CVE.ORG | w |
| NVD vulnerability detail | NVD | n |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

159306 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9362)

159307 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9363)

159340 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9407)

159341 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9410)

174916 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1210-1)

174917 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1211-1)

174919 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1238-1)

174925 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1248-1)

174938 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1301-1)

178679 Debian Security Update for linux-4.19 (DLA 2690-1)

178680 Debian Security Update for linux (DLA 2689-1)

198365 Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-4948-1)

198396 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4977-1)

198398 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4979-1)

198401 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4982-1)

198417 Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4999-1)

281307 Fedora Security Update for kernel (FEDORA-2021-21360476b6)

281308 Fedora Security Update for kernel (FEDORA-2021-d56567bdab)

281309 Fedora Security Update for kernel (FEDORA-2021-1c170a7c7c)

352274 Amazon Linux Security Advisory for kernel: ALAS2-2021-1627

352366 Amazon Linux Security Advisory for kernel: ALAS-2021-1503

352831 Amazon Linux Security Advisory for kernel: ALAC2012-2021-030

352832 Amazon Linux Security Advisory for kmod-sfc: ALAC2012-2021-031

352833 Amazon Linux Security Advisory for kmod-mlx5: ALAC2012-2021-032

353148 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-003

353159 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-001

378473 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2023:0021)

670488 EulerOS Security Update for kernel (EulerOS-SA-2021-2246)

670514 EulerOS Security Update for kernel (EulerOS-SA-2021-2272)

670578 EulerOS Security Update for kernel (EulerOS-SA-2021-2336)

670634 EulerOS Security Update for kernel (EulerOS-SA-2021-2392)

671047 EulerOS Security Update for kernel (EulerOS-SA-2021-2588)

750004 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1573-1)

750006 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1596-1)

750014 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1623-1)

750015 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1624-1)

750199 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0758-1)

750261 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0579-1)

750650 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1975-1)

750652 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1977-1)

750762 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1977-1)

750766 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1975-1)

751688 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 37 for SLE 12 SP3) (SUSE-SU-2022:0325-1)

753087 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 22 for SLE 15) (SUSE-SU-2022:0255-1)

753211 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 11 for SLE 15 SP2) (SUSE-SU-2022:0291-1)

753257 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 23 for SLE 15) (SUSE-SU-2022:0243-1)

753272 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 16 for SLE 12 SP5) (SUSE-SU-2022:0234-1)

753292 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 0 for SLE 15 SP3) (SUSE-SU-2022:0293-1)

753408 SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 15 for SLE 12 SP5) (SUSE-SU-2022:0263-1)