



CVE-2021-3743

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2021-3743 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2022-03-04 16:15:00 UTC |
| Updated | 2023-11-09 14:44:00 UTC |
| Description | An out-of-bounds (OOB) memory read flaw was found in the Qualcomm IPC router protocol in the Linux kernel. A missing s |

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|-------------------------------|--|---------|--------|---------|----------|
| Operating System | Fedoraproject | Fedora | 34 | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Operating System | Linux | Linux Kernel | 5.14 | rc6 | All | All |
| Operating System | Linux | Linux Kernel | 5.17 | - | All | All |
| Operating System | Linux | Linux Kernel | 5.17 | rc1 | All | All |
| Operating System | Linux | Linux Kernel | 5.17 | rc2 | All | All |
| Operating System | Linux | Linux Kernel | 5.17 | rc3 | All | All |
| Operating System | Linux | Linux Kernel | 5.17 | rc4 | All | All |
| Operating System | Linux | Linux Kernel | 5.17 | rc5 | All | All |
| Operating System | Linux | Linux Kernel | 5.17 | rc6 | All | All |
| Hardware | Netapp | Baseboard Management Controller H300e | - | All | All | All |
| Operating System | Netapp | Baseboard Management Controller H300e Firmware | - | All | All | All |
| Hardware | Netapp | Baseboard Management Controller H300s | - | All | All | All |
| Operating System | Netapp | Baseboard Management Controller H300s Firmware | - | All | All | All |
| Hardware | Netapp | Baseboard Management Controller H410c | - | All | All | All |
| Operating System | Netapp | Baseboard Management Controller H410c Firmware | - | All | All | All |
| Hardware | Netapp | Baseboard Management Controller H410s | - | All | All | All |

| | | | | | | |
|------------------|------------------------|--|--------|-----|-----|-----|
| Operating System | Netapp | Baseboard Management Controller H410s Firmware | - | All | All | All |
| Hardware | Netapp | Baseboard Management Controller H500e | - | All | All | All |
| Operating System | Netapp | Baseboard Management Controller H500e Firmware | - | All | All | All |
| Hardware | Netapp | Baseboard Management Controller H500s | - | All | All | All |
| Operating System | Netapp | Baseboard Management Controller H500s Firmware | - | All | All | All |
| Hardware | Netapp | Baseboard Management Controller H700e | - | All | All | All |
| Operating System | Netapp | Baseboard Management Controller H700e Firmware | - | All | All | All |
| Hardware | Netapp | Baseboard Management Controller H700s | - | All | All | All |
| Operating System | Netapp | Baseboard Management Controller H700s Firmware | - | 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 |
| Application | Oracle | Communications Cloud Native Core Binding Support Function | 22.1.3 | All | All | All |
| Application | Oracle | Communications Cloud Native Core Network Exposure Function | 22.1.1 | All | All | All |
| Application | Oracle | Communications Cloud Native Core Policy | 22.2.0 | All | All | All |

References

| Reference | Source | Link |
|---|---------|-----------------------------------|
| CVE-2021-3743 Linux Kernel Vulnerability in NetApp Products NetApp Product Security | CONFIRM | security.netapp |
| oss-security - Re: Linux kernel: qrtr: another out-of-bound Read in qrtr_endpoint_post in net/qrtr/qrtr.c | MISC | www.openwall.com |
| Red Hat Customer Portal - Access to 24x7 support and knowledge | MISC | access.redhat.com |
| kernel/git/torvalds/linux.git - Linux kernel source tree | MISC | git.kernel.org |

| | | |
|--|---------|---|
| 1997961 – (CVE-2021-3743) CVE-2021-3743 kernel: out-of-bound Read in qrtr_endpoint_post in net/qrtr/qrtr.c | MISC | bugzilla.redhat.com |
| Red Hat Customer Portal - Access to 24x7 support and knowledge | MISC | access.redhat.com |
| net: qrtr: fix another OOB Read in qrtr_endpoint_post · torvalds/linux@7e78c59 · GitHub | MISC | github.com |
| Red Hat Customer Portal - Access to 24x7 support and knowledge | MISC | access.redhat.com |
| kernel/git/netdev/net.git - Netdev Group's networking tree | MISC | git.kernel.org |
| netdev - Another out-of-bound Read in qrtr_endpoint_post in net/qrtr/qrtr.c | MISC | lists.openwall.net |
| Oracle Critical Patch Update Advisory - July 2022 | N/A | www.oracle.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

| |
|---|
| 159421 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9474) |
| 159422 Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel-container (ELSA-2021-9475) |
| 159825 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-1988) |
| 178809 Debian Security Update for linux (DSA 4978-1) |
| 178844 Debian Security Update for linux-4.19 (DLA 2785-1) |
| 179558 Debian Security Update for linux (CVE-2021-3743) |
| 198540 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5113-1) |
| 198542 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5115-1) |
| 198543 Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5117-1) |
| 198562 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5136-1) |
| 198563 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5137-1) |
| 198565 Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5137-2) |
| 240275 Red Hat Update for kernel-rt (RHSA-2022:1975) |
| 240298 Red Hat Update for kernel security (RHSA-2022:1988) |
| 377181 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2022:0022) |
| 610418 Google Pixel Android June 2022 Security Patch Missing |
| 610422 Google Android July 2022 Security Patch Missing for Huawei EMUI |
| 671134 EulerOS Security Update for kernel (EulerOS-SA-2021-2688) |

| |
|--|
| 671137 EulerOS Security Update for kernel (EulerOS-SA-2021-2713) |
| 751137 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1271-1) |
| 751160 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3179-1) |
| 751170 OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:3205-1) |
| 901158 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8921-1) |
| 906366 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (8921-2) |
| 940517 AlmaLinux Security Update for kernel (ALSA-2022:1988) |

© [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](#)