



# CVE-2022-28893

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2022-28893  |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | cve@mitre.org   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2022-04-11 05:15:00 UTC   |
| <b>Updated</b>         | 2023-05-15 18:45:00 UTC   |
| <b>Description</b>     | The SUNRPC subsystem in the Linux kernel through 5.17.2 can call xs_xprt_free before ensuring that sockets are in the int |

## 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   | 11.0    | All    | All     | All      |
| Operating System | Linux  | Linux Kernel   | All     | All    | All     | All      |
| Operating System | Linux  | Linux Kernel   | All     | 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 | Hci Compute Node                          | - | All | All | All |
| Operating System | Netapp | Hci Compute Node Firmware                 | - | All | All | All |
| Application      | Netapp | Solidfire Enterprise Sds Hci Storage Node | - | All | All | All |
| Application      | Netapp | Solidfire Hci Management Node             | - | All | All | All |

## References

| Reference  | Source  | Link   | Tags          |
|--|---------|--|---------------|
| oss-security - CVE-2022-28893: Linux kernel: Use after free in SUNRPC subsystem        | MLIST   | <a href="http://www.openwall.com">www.openwall.com</a>       |               |
| kernel/git/torvalds/linux.git - Linux kernel source tree                               | MISC    | <a href="http://git.kernel.org">git.kernel.org</a>           |               |
| CVE-2022-28893 Linux Kernel Vulnerability in NetApp Products   NetApp Product Security | CONFIRM | <a href="http://security.netapp.com">security.netapp.com</a> |               |
| oss-security - Re: CVE-2022-28893: Linux kernel: Use after free in SUNRPC subsystem    | MLIST   | <a href="http://www.openwall.com">www.openwall.com</a>       |               |
| oss-security - Re: CVE-2022-28893: Linux kernel: Use after free in SUNRPC subsystem    | MLIST   | <a href="http://www.openwall.com">www.openwall.com</a>       |               |
| Debian -- Security Information -- DSA-5161-1 linux                                     | DEBIAN  | <a href="http://www.debian.org">www.debian.org</a>           |               |
| CVE Program record   | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                 | canonical     |
| NVD vulnerability detail   | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>               | canonical, ar |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

|  |
|--|
| <a href="#">160210</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2022-7683)                     |
| <a href="#">160270</a> Oracle Enterprise Linux Security Update for kernel (ELSA-2022-8267)                     |
| <a href="#">179371</a> Debian Security Update for linux (DSA 5161-1)   |
| <a href="#">184635</a> Debian Security Update for linux (CVE-2022-28893)                                       |
| <a href="#">198880</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5544-1)              |
| <a href="#">198894</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5566-1)              |
| <a href="#">198895</a> Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5562-1)              |
| <a href="#">198897</a> Ubuntu Security Notification for Linux kernel (Intel IoTG) Vulnerabilities (USN-5564-1) |
| <a href="#">198911</a> Ubuntu Security Notification for Linux kernel (Azure CVM) Vulnerabilities (USN-5582-1)  |
| <a href="#">240815</a> Red Hat Update for kernel-rt (RHSA-2022:7444)   |
| <a href="#">240817</a> Red Hat Update for kernel security (RHSA-2022:7683)                                     |
| <a href="#">240869</a> Red Hat Update for kernel-rt (RHSA-2022:7933)   |

|   |
|---|
| 240904 Red Hat Update for kernel security (RHSA-2022:8267)                              |
| 242890 Red Hat Update for kernel (RHSA-2024:0724)                                       |
| 353960 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.10-2022-014            |
| 353962 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.4-2022-026             |
| 353964 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2022-001            |
| 354327 Amazon Linux Security Advisory for kernel : ALAS2022-2022-083                    |
| 354468 Amazon Linux Security Advisory for kernel : ALAS2022-2022-185                    |
| 354542 Amazon Linux Security Advisory for kernel : ALAS-2022-185                        |
| 355199 Amazon Linux Security Advisory for kernel : ALAS2023-2023-070                    |
| 355565 Amazon Linux Security Advisory for kernel : ALAS2KERNEL-5.15-2023-023            |
| 377117 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0158)      |
| 6140415 AWS Bottlerocket Security Update for kernel (GHSA-m63c-5pgq-vm26)               |
| 752126 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1687-1) |
| 752242 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2104-1) |
| 753176 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1676-1) |
| 753299 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:1669-1) |
| 900795 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9329)        |
| 901119 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9332)        |
| 902073 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9332-1)      |
| 902200 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9329-1)      |
| 906016 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9329-2)      |
| 906315 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9332-2)      |
| 940732 AlmaLinux Security Update for kernel (ALSA-2022:7683)                            |
| 940766 AlmaLinux Security Update for kernel-rt (ALSA-2022:7444)                         |
| 940798 AlmaLinux Security Update for kernel (ALSA-2022:8267)                            |
| 940843 AlmaLinux Security Update for kernel-rt (ALSA-2022:7933)                         |
| 960176 Rocky Linux Security Update for kernel-rt (RLSA-2022:7444)                       |
| 960184 Rocky Linux Security Update for kernel (RLSA-2022:7683)                          |

© [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](#)**