# CVE-2022-1998

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2022-1998 |
| **State** | PUBLIC |
| **Assigner** | secalert@redhat.com |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2022-06-09 15:15:00 UTC |
| **Updated** | 2023-05-16 10:50:00 UTC |
| **Description** | A use after free in the Linux kernel File System notify functionality was found in the way user triggers copy_info_records_to_ |

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Fedoraproject | Fedora | 35 | All | All | All |
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Operating System | Linux | Linux Kernel | 5.17 | rc1 | All | All |
| Operating System | Linux | Linux Kernel | 5.17 | rc2 | 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 | H500s | - | All | All | All |
| Operating System | Netapp | H500s Firmware | - | All | All | All |
| Hardware | Netapp | H700s | - | All | All | All |
| Operating System | Netapp | H700s Firmware | - | All | All | All |
| Operating System | Redhat | Enterprise Linux | 9.0 | All | All | All |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| CVE-2022-1998 Linux Kernel Vulnerability in NetApp Products \| NetApp Product Security | CONFIRM | security.netapp.com | |
| kernel/git/torvalds/linux.git - Linux kernel source tree | MISC | git.kernel.org | |
| oss-sec: Linux kernel: erroneous error handling after fd_install() | MISC | seclists.org | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, ana |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

- 160270 Oracle Enterprise Linux Security Update for kernel (ELSA-2022-8267)
- 179366 Debian Security Update for linux (CVE-2022-1998)
- 240869 Red Hat Update for kernel-rt (RHSA-2022:7933)
- 240904 Red Hat Update for kernel security (RHSA-2022:8267)
- 376925 Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX3-SA-2022:0125)
- 752370 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2520-1)
- 753148 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2022:2615-1)
- 902179 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9911)
- 902181 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9917)
- 902400 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9917-1)
- 902502 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9911-1)
- 906053 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9911-2)
- 906383 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (9917-2)
- 940798 AlmaLinux Security Update for kernel (ALSA-2022:8267)
- 940843 AlmaLinux Security Update for kernel-rt (ALSA-2022:7933)

© 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 registred 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.

**Free CVE JSON API** cve.report/api

**CVE.report and Source URL Uptime Status** status.cve.report