



# CVE-2020-35508

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2020-35508   |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | secalert@redhat.com  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2021-03-26 17:15:00 UTC  |
| <b>Updated</b>         | 2023-02-12 23:41:00 UTC  |
| <b>Description</b>     | A flaw possibility of race condition and incorrect initialization of the process id was found in the Linux kernel child/parent pro |

## Risk And Classification

**Problem Types:** CWE-665

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                 | Product  | Version | Update | Edition | Language |
|------------------|------------------------|--|---------|--------|---------|----------|
| Operating System | <a href="#">Linux</a>  | <a href="#">Linux Kernel</a>                             | All     | All    | All     | All      |
| Operating System | <a href="#">Linux</a>  | <a href="#">Linux Kernel</a>                             | 5.12    | -      | All     | All      |
| Operating System | <a href="#">Linux</a>  | <a href="#">Linux Kernel</a>                             | 5.12    | rc1    | All     | All      |
| Operating System | <a href="#">Linux</a>  | <a href="#">Linux Kernel</a>                             | 5.12    | rc2    | All     | All      |
| Operating System | <a href="#">Linux</a>  | <a href="#">Linux Kernel</a>                             | 5.12    | rc3    | All     | All      |
| Operating System | <a href="#">Linux</a>  | <a href="#">Linux Kernel</a>                             | 5.12    | rc4    | All     | All      |
| Hardware         | <a href="#">Netapp</a> | <a href="#">A700s</a>                                    | -       | All    | All     | All      |
| Operating System | <a href="#">Netapp</a> | <a href="#">A700s Firmware</a>                           | -       | All    | All     | All      |
| Hardware         | <a href="#">Netapp</a> | <a href="#">Aff A400</a>                                 | -       | All    | All     | All      |
| Operating System | <a href="#">Netapp</a> | <a href="#">Aff A400 Firmware</a>                        | -       | All    | All     | All      |
| Operating System | <a href="#">Netapp</a> | <a href="#">Brocade Fabric Operating System Firmware</a> | -       | All    | All     | All      |
| Hardware         | <a href="#">Netapp</a> | <a href="#">Fas8300</a>                                  | -       | All    | All     | All      |
| Operating System | <a href="#">Netapp</a> | <a href="#">Fas8300 Firmware</a>                         | -       | All    | All     | All      |
| Hardware         | <a href="#">Netapp</a> | <a href="#">Fas8700</a>                                  | -       | All    | All     | All      |
| Operating System | <a href="#">Netapp</a> | <a href="#">Fas8700 Firmware</a>                         | -       | All    | All     | All      |
| Hardware         | <a href="#">Netapp</a> | <a href="#">H300e</a>                                    | -       | All    | All     | All      |
| Operating System | <a href="#">Netapp</a> | <a href="#">H300e Firmware</a>                           | -       | 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 | H610c            | -   | All | All | All |
| Operating System | Netapp | H610c Firmware   | -   | All | All | All |
| Hardware         | Netapp | H610s            | -   | All | All | All |
| Operating System | Netapp | H610s Firmware   | -   | All | All | All |
| Hardware         | Netapp | H615c            | -   | All | All | All |
| Operating System | Netapp | H615c 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 |
| Operating System | Redhat | Enterprise Linux | 8.0 | All | All | All |

## References

| Reference  | Source |
|--|--------|
| fork: fix copy_process(CLONE_PARENT) race with the exiting ->real_parent · torvalds/linux@b4e0044 · GitHub                 | MISC   |
| CVE-2020-35508 Linux Kernel Vulnerability in NetApp Products   NetApp Product Security                                     | CONF   |
| 1902724 – (CVE-2020-35508) CVE-2020-35508 kernel: fork: fix copy_process(CLONE_PARENT) race with the exiting ->real_parent | MISC   |
| Red Hat Customer Portal - Access to 24x7 support and knowledge   | MISC   |
| Red Hat Customer Portal - Access to 24x7 support and knowledge   | MISC   |
| Red Hat Customer Portal - Access to 24x7 support and knowledge   | MISC   |
| Red Hat Customer Portal - Access to 24x7 support and knowledge   | MISC   |
| Red Hat Customer Portal - Access to 24x7 support and knowledge   | MISC   |
| CVE Program record   | CVE.C  |
| NVD vulnerability detail   | NVD    |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[159175](#) Oracle Enterprise Linux Security Update for Unbreakable Enterprise kernel (ELSA-2021-9215)

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

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

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

[239501](#) Red Hat Update for kernel-rt (RHSA-2021:2719) (Sequoia)

[239502](#) Red Hat Update for kernel (RHSA-2021:2718) (Sequoia)

[390225](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for kernel (OVMSA-2021-0016)

[900100](#) CBL-Mariner Linux Security Update for kernel 5.10.52.1

[900305](#) CBL-Mariner Linux Security Update for kernel 5.10.57.1

[900320](#) CBL-Mariner Linux Security Update for kernel 5.10.60.1

[901953](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6528-1)

[903256](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4030)

[905857](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4030-1)

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

© [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](#)