



CVE-2021-38201

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2021-38201 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2021-08-08 20:15:00 UTC |
| Updated | 2021-10-07 20:39:00 UTC |
| Description | net/sunrpc/xdr.c in the Linux kernel before 5.13.4 allows remote attackers to cause a denial of service (xdr_set_page_base |

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------|---------------------|---------|--------|---------|----------|
| Operating System | Linux | Linux Kernel | All | All | All | All |
| Application | Netapp | Element Software | - | All | All | All |
| Operating System | Netapp | Hci Bootstrap Os | - | All | All | All |
| Hardware | Netapp | Hci Compute Node | - | All | All | All |
| Application | Netapp | Hci Management Node | - | All | All | All |
| Hardware | Netapp | Hci Storage Node | - | All | All | All |
| Application | Netapp | Solidfire | - | All | All | All |

References

| Reference | Source | Link |
|---|---------|---|
| August 2021 Linux Kernel 5.13.4 Vulnerabilities in NetApp Products NetApp Product Security | CONFIRM | security.netapp.com |
| sunrpc: Avoid a KASAN slab-out-of-bounds bug in xdr_set_page_base() · torvalds/linux@6d1c0f3 · GitHub | MISC | github.com |
| cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.13.4 | MISC | cdn.kernel.org |
| 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

[159379](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2021-3447)

[198515](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5092-1)

[198523](#) Ubuntu Security Notification for Linux kernel Vulnerabilities (USN-5092-2)

[198524](#) Ubuntu Security Notification for Linux kernel (OEM) Vulnerabilities (USN-5096-1)

[239611](#) Red Hat Update for kernel (RHSA-2021:3447)

[239618](#) Red Hat Update for kernel-rt (RHSA-2021:3440)

[900294](#) CBL-Mariner Linux Security Update for kernel 5.10.52.1

[900304](#) CBL-Mariner Linux Security Update for kernel 5.10.57.1

[900319](#) CBL-Mariner Linux Security Update for kernel 5.10.60.1

[901070](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6585-1)

[902798](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5076)

[906138](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (5076-1)

[940058](#) AlmaLinux Security Update for kernel (ALSA-2021:3447)

[960014](#) Rocky Linux Security Update for kernel-rt (RLSA-2021:3440)

[960048](#) Rocky Linux Security Update for kernel (RLSA-2021:3447)

© [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](#)