



# CVE-2021-33200

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2021-33200   |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@mitre.org  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2021-05-27 13:15:00 UTC  |
| <b>Updated</b>         | 2023-11-07 03:35:00 UTC  |
| <b>Description</b>     | kernel/bpf/verifier.c in the Linux kernel through 5.12.7 enforces incorrect limits for pointer arithmetic operations, aka CID-bb |

## Risk And Classification

### Problem Types: CWE-787

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                        | Product                        | Version | Update | Edition | Language |
|------------------|-------------------------------|--------------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>         | 33      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a> | <a href="#">Fedora</a>         | 34      | All    | All     | All      |
| 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>   | All     | All    | All     | All      |
| Application      | <a href="#">Netapp</a>        | <a href="#">Cloud Backup</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         | <a href="#">Netapp</a>        | <a href="#">H300s</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Netapp</a>        | <a href="#">H300s Firmware</a> | -       | All    | All     | All      |
| Hardware         | <a href="#">Netapp</a>        | <a href="#">H410s</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Netapp</a>        | <a href="#">H410s Firmware</a> | -       | All    | All     | All      |
| Hardware         | <a href="#">Netapp</a>        | <a href="#">H500e</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Netapp</a>        | <a href="#">H500e Firmware</a> | -       | All    | All     | All      |
| Hardware         | <a href="#">Netapp</a>        | <a href="#">H500s</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Netapp</a>        | <a href="#">H500s Firmware</a> | -       | All    | All     | All      |
| Hardware         | <a href="#">Netapp</a>        | <a href="#">H700e</a>          | -       | All    | All     | All      |
| Operating System | <a href="#">Netapp</a>        | <a href="#">H700e Firmware</a> | -       | All    | All     | All      |

|                  |                        |   |   |     |     |     |
|------------------|------------------------|---|---|-----|-----|-----|
| Hardware         | <a href="#">Netapp</a> | <a href="#">H700s</a>                                     | - | All | All | All |
| Operating System | <a href="#">Netapp</a> | <a href="#">H700s Firmware</a>                            | - | All | All | All |
| Application      | <a href="#">Netapp</a> | <a href="#">Solidfire Baseboard Management Controller</a> | - | All | All | All |
| Application      | <a href="#">Netapp</a> | <a href="#">Solidfire Hci Management Node</a>             | - | All | All | All |

## References

### Reference

[SECURITY] Fedora 34 Update: kernel-5.12.8-300.fc34 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 33 Update: kernel-5.12.8-200.fc33 - package-announce - Fedora Mailing-Lists

[CVE-2021-33200 Linux Kernel Vulnerability in NetApp Products | NetApp Product Security](#)

[SECURITY] Fedora 33 Update: kernel-5.12.8-200.fc33 - package-announce - Fedora Mailing-Lists

oss-security - [CVE-2021-33200] Linux kernel enforcing incorrect limits for pointer arithmetic operations by BPF verifier can be abused to perform

[SECURITY] Fedora 34 Update: kernel-5.12.8-300.fc34 - package-announce - Fedora Mailing-Lists

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[159492](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2021-4356)

[180538](#) Debian Security Update for linux (CVE-2021-33200)

[198402](#) Ubuntu Security Notification for Linux kernel (OEM) vulnerabilities (USN-4983-1)

[198416](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4997-1)

[198417](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4999-1)

[198418](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-5000-1)

[198425](#) Ubuntu Security Notification for Linux kernel (KVM) vulnerabilities (USN-5000-2)

[198426](#) Ubuntu Security Notification for Linux kernel (KVM) vulnerabilities (USN-4997-2)

[198459](#) Ubuntu Security Notification for Linux, Linux-aws, Linux-aws-hwe, Linux-azure, Linux-azure-4.15, Linux-gcp, (USN-5018-1)

[239816](#) Red Hat Update for kernel security (RHSA-2021:4356)

[239879](#) Red Hat Update for kernel-rt (RHSA-2021:4140)

[281096](#) Fedora Security Update for kernel (FEDORA-2021-646098b5b8)

[281097](#) Fedora Security Update for kernel (FEDORA-2021-0b35886add)

|  |
|--|
| <a href="#">281487</a> Fedora Security Update for kernel (FEDORA-2021-646098b5b8)  |
| <a href="#">281488</a> Fedora Security Update for kernel (FEDORA-2021-0b35886add)  |
| <a href="#">352461</a> Amazon Linux Security Advisory for kernel: ALAS2-2021-1675  |
| <a href="#">352475</a> Amazon Linux Security Advisory for kernel: ALAS-2021-1516   |
| <a href="#">352498</a> Amazon Linux Security Advisory for kernel-livepatch: ALAS2LIVEPATCH-2021-054                                    |
| <a href="#">610384</a> Google Pixel Android December 2021 Security Patch Missing   |
| <a href="#">670514</a> EulerOS Security Update for kernel (EulerOS-SA-2021-2272)   |
| <a href="#">670543</a> EulerOS Security Update for kernel (EulerOS-SA-2021-2301)   |
| <a href="#">670796</a> EulerOS Security Update for kernel (EulerOS-SA-2021-2554)   |
| <a href="#">750117</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1891-1)                                |
| <a href="#">750118</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1890-1)                                |
| <a href="#">750121</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1888-1)                                |
| <a href="#">750125</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1887-1)                                |
| <a href="#">750126</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1889-1)                                |
| <a href="#">750139</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1913-1)                                |
| <a href="#">750140</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1912-1)                                |
| <a href="#">750171</a> OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0843-1)   |
| <a href="#">750650</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1975-1)                                |
| <a href="#">750652</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1977-1)                                |
| <a href="#">750674</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 18 for SLE 12 SP5) (SUSE-SU-2021:2020-1) |
| <a href="#">750676</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 13 for SLE 15 SP2) (SUSE-SU-2021:2027-1) |
| <a href="#">750678</a> SUSE Enterprise Linux Security Update for the Linux Kernel (Live Patch 24 for SLE 15) (SUSE-SU-2021:2057-1)     |
| <a href="#">750741</a> OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:0947-1)   |
| <a href="#">750762</a> OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1977-1)   |
| <a href="#">750766</a> OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1975-1)   |
| <a href="#">750864</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2421-1)                                |
| <a href="#">750868</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2427-1)                                |
| <a href="#">750869</a> SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:2422-1)                                |
| <a href="#">750877</a> OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:2427-1)   |

|   |
|---|
| 755988 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0975-1) |
| 756005 SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2024:0925-1) |
| 900096 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                           |
| 901733 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (6563-1)      |
| 902919 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4244)        |
| 905960 Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (4244-1)      |
| 940265 AlmaLinux Security Update for kernel (ALSA-2021:4356)                            |

© [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](#)