



# CVE-2021-20268

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

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2021-20268   |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | secalert@redhat.com  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2021-03-09 18:15:00 UTC  |
| <b>Updated</b>         | 2023-11-07 03:29:00 UTC  |
| <b>Description</b>     | An out-of-bounds access flaw was found in the Linux kernel's implementation of the eBPF code verifier in the way a user ru |

## Risk And Classification

**Problem Types:** CWE-190

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor | Product                      | Version | Update | Edition | Language |
|------------------|--------|------------------------------|---------|--------|---------|----------|
| Operating System | Linux  | Linux Kernel                 | All     | All    | All     | All      |
| Operating System | Redhat | Enterprise Linux             | 8.0     | All    | All     | All      |
| Application      | Redhat | Openshift Container Platform | 4.4     | All    | All     | All      |
| Application      | Redhat | Openshift Container Platform | 4.5     | All    | All     | All      |
| Application      | Redhat | Openshift Container Platform | 4.6     | All    | All     | All      |
| Application      | Redhat | Openshift Container Platform | 4.7     | All    | All     | All      |

## References

| Reference  | Source  | Link  | Tags           |
|--|---------|---|----------------|
| 1923816 – (CVE-2021-20268) CVE-2021-20268 kernel: eBPF Improper Input Validation       | MISC    | <a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a> | Issue Tracking |
| CVE-2021-20268 Linux Kernel Vulnerability in NetApp Products   NetApp Product Security | CONFIRM | <a href="https://security.netapp.com">security.netapp.com</a> |                |
| [PATCH] bpf: Fix integer overflow in argument calculation for bpf_map_area_alloc       |         | <a href="https://lore.kernel.org">lore.kernel.org</a>         |                |
| [PATCH] bpf: Fix integer overflow in argument calculation for bpf_map_area_alloc       | MISC    | <a href="https://lore.kernel.org">lore.kernel.org</a>         | Patch, Vendor  |
| CVE Program record   | CVE.ORG | <a href="https://www.cve.org">www.cve.org</a>                 | canonical      |
| NVD vulnerability detail   | NVD     | <a href="https://nvd.nist.gov">nvd.nist.gov</a>               | canonical, ar  |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[180162](#) Debian Security Update for linux (CVE-2021-20268)

[198326](#) Ubuntu Security Notification for Linux kernel vulnerabilities (USN-4910-1)

[610418](#) Google Pixel Android June 2022 Security Patch Missing

[610422](#) Google Android July 2022 Security Patch Missing for Huawei EMUI

[750650](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1975-1)

[750652](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2021:1977-1)

[750762](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1977-1)

[750766](#) OpenSUSE Security Update for the Linux Kernel (openSUSE-SU-2021:1975-1)

[900098](#) CBL-Mariner Linux Security Update for kernel 5.4.91

[903038](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (3987)

© [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](#)