



# CVE-2021-3200

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

## Summary

<b>CVE</b>	CVE-2021-3200
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-05-18 17:15:00 UTC
<b>Updated</b>	2022-07-30 03:45:00 UTC
<b>Description</b>	Buffer overflow vulnerability in libsolv 2020-12-13 via the Solver * testcase_read(Pool *pool, FILE *fp, const char *testcase,

## Risk And Classification

**Problem Types:** CWE-120

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Opensuse</a>	<a href="#">Libsolv</a>	All	All	All	All
Application	<a href="#">Oracle</a>	<a href="#">Communications Cloud Native Core Policy</a>	1.15.0	All	All	All

## References

Reference	Source	Link	Tags
Oracle Critical Patch Update Advisory - April 2022	MISC	<a href="http://www.oracle.com">www.oracle.com</a>	
libsolv "testcase_read" function a heap overflow vulnerability · Issue #416 · openSUSE/libsolv · GitHub	MISC	<a href="https://github.com">github.com</a>	
PoC/PoC-testcase_read-2334 at master · yangjiageng/PoC · GitHub	MISC	<a href="https://github.com">github.com</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[159509](#) Oracle Enterprise Linux Security Update for libsolv (ELSA-2021-4408)

[180295](#) Debian Security Update for libsolv (CVE-2021-3200)

[2021-07-01](#) Debian Security Update for libsolv (DUSAP-2021-4408)

<a href="#">239819</a> Red Hat Update for libsolv (RHSA-2021:4408)
<a href="#">240566</a> Red Hat Update for Satellite 6.11 Release (RHSA-2022:5498)
<a href="#">354398</a> Amazon Linux Security Advisory for libsolv : ALAS2022-2022-167
<a href="#">354491</a> Amazon Linux Security Advisory for libsolv : ALAS2022-2022-093
<a href="#">355231</a> Amazon Linux Security Advisory for libsolv : ALAS2023-2023-013
<a href="#">670713</a> EulerOS Security Update for libsolv (EulerOS-SA-2021-2471)
<a href="#">670748</a> EulerOS Security Update for libsolv (EulerOS-SA-2021-2506)
<a href="#">670775</a> EulerOS Security Update for libsolv (EulerOS-SA-2021-2533)
<a href="#">670799</a> EulerOS Security Update for libsolv (EulerOS-SA-2021-2557)
<a href="#">670950</a> EulerOS Security Update for libsolv (EulerOS-SA-2021-2593)
<a href="#">750732</a> SUSE Enterprise Linux Security Update for libsolv (SUSE-SU-2021:2180-1)
<a href="#">900281</a> CBL-Mariner Linux Security Update for libsolv 0.7.7
<a href="#">902812</a> Common Base Linux Mariner (CBL-Mariner) Security Update for libsolv (4205)
<a href="#">940163</a> AlmaLinux Security Update for libsolv (ALSA-2021:4408)
<a href="#">960505</a> Rocky Linux Security Update for Satellite (RLSA-2022:5498)
<a href="#">960819</a> Rocky Linux Security Update for libsolv (RLSA-2021:4408)

© [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](#)