



# CVE-2021-36084

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-36084
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-07-01 03:15:00 UTC
<b>Updated</b>	2023-11-07 03:36:00 UTC
<b>Description</b>	The CIL compiler in SELinux 3.2 has a use-after-free in __cil_verify_classperms (called from __cil_verify_classpermission a

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	35	All	All	All
Operating System	<a href="#">Selinux Project</a>	<a href="#">Selinux</a>	3.2	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 35 Update: libsepol-3.3-2.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lists.fedoraproj</a>
[SECURITY] Fedora 35 Update: libsepol-3.3-2.fc35 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproj</a>
31065 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	MISC	<a href="#">bugs.chromium</a>
libsepol/cil: Destroy classperms list when resetting classpermission · SELinuxProject/selinux@f34d3d3 · GitHub	MISC	<a href="#">github.com</a>
oss-fuzz-vulns/OSV-2021-417.yaml at main · google/oss-fuzz-vulns · GitHub	MISC	<a href="#">github.com</a>
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[159521](#) Oracle Enterprise Linux Security Update for libsepol (ELSA-2021-4513)

<a href="#">184749</a> Debian Security Update for libsepol (CVE-2021-36084)
<a href="#">198754</a> Ubuntu Security Notification for libsepol Vulnerabilities (USN-5391-1)
<a href="#">239808</a> Red Hat Update for libsepol (RHSA-2021:4513)
<a href="#">282153</a> Fedora Security Update for libsepol (FEDORA-2021-67efe88c29)
<a href="#">354312</a> Amazon Linux Security Advisory for libsepol : ALAS2022-2022-030
<a href="#">354524</a> Amazon Linux Security Advisory for libsepol : ALAS2022-2022-170
<a href="#">354704</a> Amazon Linux Security Advisory for libsepol : ALAS2022-2022-208
<a href="#">355129</a> Amazon Linux Security Advisory for libsepol : ALAS2023-2023-017
<a href="#">356236</a> Amazon Linux Security Advisory for libsepol : ALASSELINUX-NG-2023-001
<a href="#">356437</a> Amazon Linux Security Advisory for libsepol : ALAS2-2023-2307
<a href="#">356590</a> Amazon Linux Security Advisory for libsepol : ALAS2SELINUX-NG-2023-001
<a href="#">591406</a> Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)
<a href="#">671260</a> EulerOS Security Update for libsepol (EulerOS-SA-2022-1174)
<a href="#">671274</a> EulerOS Security Update for libsepol (EulerOS-SA-2022-1245)
<a href="#">671334</a> EulerOS Security Update for libsepol (EulerOS-SA-2022-1257)
<a href="#">671341</a> EulerOS Security Update for libsepol (EulerOS-SA-2022-1273)
<a href="#">671370</a> EulerOS Security Update for libsepol (EulerOS-SA-2022-1309)
<a href="#">671373</a> EulerOS Security Update for libsepol (EulerOS-SA-2022-1293)
<a href="#">940148</a> AlmaLinux Security Update for libsepol (ALSA-2021:4513)
<a href="#">960253</a> Rocky Linux Security Update for libsepol (RLSA-2021:4513)

© [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](#)**