



CVE-2021-36087

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2021-36087
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-07-01 03:15:00 UTC
Updated	2023-11-07 03:36:00 UTC
Description	The CIL compiler in SELinux 3.2 has a heap-based buffer over-read in ebitmap_match_any (called indirectly from cil_check

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Selinux Project	Selinux	3.2	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 35 Update: libsepol-3.3-2.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.
secilc/docs: Update the CIL documentation for various blocks · SELinuxProject/selinux@bad0a74 · GitHub	MISC	github.com
oss-fuzz-vulns/OSV-2021-585.yaml at main · google/oss-fuzz-vulns · GitHub	MISC	github.com
libsepol/cil: Check for statements not allowed in optional blocks · SELinuxProject/selinux@340f0eb · GitHub	MISC	github.com
libsepol CVE patch issue		lore.kernel.org
[SECURITY] Fedora 35 Update: libsepol-3.3-2.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.
libsepol CVE patch issue	MISC	lore.kernel.org
32675 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	MISC	bugs.chromium.or
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

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

183120 Debian Security Update for libsepol (CVE-2021-36087)

198754 Ubuntu Security Notification for libsepol Vulnerabilities (USN-5391-1)

239808 Red Hat Update for libsepol (RHSA-2021:4513)

282153 Fedora Security Update for libsepol (FEDORA-2021-67efe88c29)

354312 Amazon Linux Security Advisory for libsepol : ALAS2022-2022-030

354524 Amazon Linux Security Advisory for libsepol : ALAS2022-2022-170

354704 Amazon Linux Security Advisory for libsepol : ALAS2022-2022-208

355129 Amazon Linux Security Advisory for libsepol : ALAS2023-2023-017

356236 Amazon Linux Security Advisory for libsepol : ALASSELINUX-NG-2023-001

356437 Amazon Linux Security Advisory for libsepol : ALAS2-2023-2307

356590 Amazon Linux Security Advisory for libsepol : ALAS2SELINUX-NG-2023-001

591406 Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)

671274 EulerOS Security Update for libsepol (EulerOS-SA-2022-1245)

671334 EulerOS Security Update for libsepol (EulerOS-SA-2022-1257)

671370 EulerOS Security Update for libsepol (EulerOS-SA-2022-1309)

671373 EulerOS Security Update for libsepol (EulerOS-SA-2022-1293)

940148 AlmaLinux Security Update for libsepol (ALSA-2021:4513)

960253 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](#)