



CVE-2023-2602

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2023-2602 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2023-06-06 20:15:00 UTC |
| Updated | 2023-11-30 05:15:00 UTC |
| Description | A vulnerability was found in the pthread_create() function in libcap. This issue may allow a malicious actor to use cause _r |

Risk And Classification

Problem Types: CWE-401

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|--------------------------------|----------------------------------|---------|--------|---------|----------|
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |
| Operating System | Debian | Debian Linux | 11.0 | All | All | All |
| Operating System | Debian | Debian Linux | 12.0 | All | All | All |
| Operating System | Fedoraproject | Fedora | 37 | All | All | All |
| Operating System | Fedoraproject | Fedora | 38 | All | All | All |
| Application | Libcap Project | Libcap | 2.66 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 8.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 9.0 | All | All | All |

References

| Reference | Source | Link | Tags |
|---|--------|---|------|
| 2209114 - (CVE-2023-2602) CVE-2023-2602 libcap: Memory Leak on pthread_create() Error | MISC | bugzilla.redhat.com | |
| www.x41-dsec.de/static/reports/X41-libcap-Code-Review-2023-OSTIF-Final-Report... | MISC | www.x41-dsec.de | |
| FEDORA-2023-5911638116 | | lists.fedoraproject.org | |
| FEDORA-2023-ad944c2d34 | | lists.fedoraproject.org | |

| | | | |
|--------------------------|---------|--|---------|
| CVE Program record | CVE.ORG | www.cve.org | canonic |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonic |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

| |
|---|
| 160856 Oracle Enterprise Linux Security Update for libcap (ELSA-2023-4524) |
| 182594 Debian Security Update for libcap2 (CVE-2023-2602) |
| 199419 Ubuntu Security Notification for libcap2 Vulnerabilities (USN-6166-1) |
| 241931 Red Hat Update for libcap (RHSA-2023:4524) |
| 242600 Red Hat Update for libcap (RHSA-2023:7400) |
| 284778 Fedora Security Update for libcap (FEDORA-2023-5911638116) |
| 285129 Fedora Security Update for libcap (FEDORA-2023-ad944c2d34) |
| 355409 Amazon Linux Security Advisory for libcap : ALAS2023-2023-195 |
| 355596 Amazon Linux Security Advisory for libcap : ALAS2-2023-2136 |
| 503009 Alpine Linux Security Update for libcap |
| 503010 Alpine Linux Security Update for libcap |
| 503012 Alpine Linux Security Update for libcap |
| 6140390 AWS Bottlerocket Security Update for libcap (GHSA-8m3j-6pg3-5pcf) |
| 673624 EulerOS Security Update for libcap (EulerOS-SA-2023-2690) |
| 674077 EulerOS Security Update for libcap (EulerOS-SA-2023-2648) |
| 907033 Common Base Linux Mariner (CBL-Mariner) Security Update for libcap (27064-1) |
| 941220 AlmaLinux Security Update for libcap (ALSA-2023:4524) |
| 941246 AlmaLinux Security Update for libcap (ALSA-2023:5071) |

© [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](#).

Free CVE JSON API cve.report/api

