



# CVE-2021-4115

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

## Summary

|                        |   |
|------------------------|---|
| <b>CVE</b>             | CVE-2021-4115   |
| <b>State</b>           | PUBLIC  |
| <b>Assigner</b>        | secalert@redhat.com   |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback  |
| <b>Published</b>       | 2022-02-21 22:15:00 UTC   |
| <b>Updated</b>         | 2023-11-07 03:40:00 UTC   |
| <b>Description</b>     | There is a flaw in polkit which can allow an unprivileged user to cause polkit to crash, due to process file descriptor exhaust |

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

| Type             | Vendor                         | Product                                   | Version | Update | Edition | Language |
|------------------|--------------------------------|---|---------|--------|---------|----------|
| Operating System | <a href="#">Canonical</a>      | <a href="#">Ubuntu Linux</a>              | 20.04   | All    | All     | All      |
| Operating System | <a href="#">Canonical</a>      | <a href="#">Ubuntu Linux</a>              | 21.10   | All    | All     | All      |
| Operating System | <a href="#">Debian</a>         | <a href="#">Debian Linux</a>              | 11.0    | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a>  | <a href="#">Fedora</a>                    | 34      | All    | All     | All      |
| Operating System | <a href="#">Fedoraproject</a>  | <a href="#">Fedora</a>                    | 35      | All    | All     | All      |
| Application      | <a href="#">Oracle</a>         | <a href="#">Zfs Storage Appliance Kit</a> | 8.8     | All    | All     | All      |
| Application      | <a href="#">Polkit Project</a> | <a href="#">Polkit</a>                    | 0.117   | All    | All     | All      |
| Operating System | <a href="#">Redhat</a>         | <a href="#">Enterprise Linux</a>          | 8.0     | All    | All     | All      |

## References

| Reference   | Source | Link                         |
|---|--------|------------------------------|
| polkit File Descriptor Exhaustion ~ Packet Storm  | MISC   | <a href="#">packetstorr</a>  |
| [SECURITY] Fedora 34 Update: polkit-0.117-3.fc34.3 - package-announce - Fedora Mailing-Lists                        |        | <a href="#">lists.fedora</a> |
| file descriptor exhaustion (GHSL-2021-077) (!6) · Merge requests · Red Hat / centos-stream / rpms / polkit · GitLab | MISC   | <a href="#">gitlab.com</a>   |
| Red Hat Customer Portal - Access to 24x7 support and knowledge  | MISC   | <a href="#">access.red</a>   |
| GHSL-2021-077: file descriptor exhaustion in polkit (#141) · Issues · polkit / polkit · GitLab                      | MISC   | <a href="#">gitlab.freed</a> |
| [SECURITY] Fedora 34 Update: polkit-0.117-3.fc34.3 - package-announce - Fedora Mailing-Lists                        | FEDORA | <a href="#">lists.fedora</a> |

|   |         |  |
|---|---------|--|
| Oracle Critical Patch Update Advisory - July 2022 | N/A     | <a href="http://www.oracle.com">www.oracle.com</a> |
| CVE Program record                                | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>       |
| NVD vulnerability detail                          | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>     |

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

|  |
|--|
| <a href="#">159767</a> Oracle Enterprise Linux Security Update for polkit (ELSA-2022-1546)               |
| <a href="#">182178</a> Debian Security Update for policykit-1 (CVE-2021-4115)                            |
| <a href="#">198684</a> Ubuntu Security Notification for PolicyKit Vulnerability (USN-5304-1)             |
| <a href="#">240236</a> Red Hat Update for polkit (RHSA-2022:1546)  |
| <a href="#">282407</a> Fedora Security Update for polkit (FEDORA-2022-353b7254fd)                        |
| <a href="#">282456</a> Fedora Security Update for polkit (FEDORA-2022-5e6d5fe680)                        |
| <a href="#">296063</a> Oracle Solaris 11.4 Support Repository Update (SRU) 45.119.2 Missing (CPUAPR2022) |
| <a href="#">354281</a> Amazon Linux Security Advisory for polkit : ALAS2022-2022-097                     |
| <a href="#">354367</a> Amazon Linux Security Advisory for polkit : ALAS2022-2022-220                     |
| <a href="#">354415</a> Amazon Linux Security Advisory for polkit : ALAS2022-2022-102                     |
| <a href="#">354564</a> Amazon Linux Security Advisory for polkit : ALAS-2022-220                         |
| <a href="#">355263</a> Amazon Linux Security Advisory for polkit : ALAS2023-2023-026                     |
| <a href="#">377353</a> Alibaba Cloud Linux Security Update for polkit (ALINUX3-SA-2022:0032)             |
| <a href="#">671606</a> EulerOS Security Update for polkit (EulerOS-SA-2022-1580)                         |
| <a href="#">671738</a> EulerOS Security Update for polkit (EulerOS-SA-2022-1796)                         |
| <a href="#">671752</a> EulerOS Security Update for polkit (EulerOS-SA-2022-1813)                         |
| <a href="#">671790</a> EulerOS Security Update for polkit (EulerOS-SA-2022-1874)                         |
| <a href="#">671808</a> EulerOS Security Update for polkit (EulerOS-SA-2022-1850)                         |
| <a href="#">751732</a> SUSE Enterprise Linux Security Update for polkit (SUSE-SU-2022:0524-1)            |
| <a href="#">751740</a> OpenSUSE Security Update for polkit (openSUSE-SU-2022:0525-1)                     |
| <a href="#">751982</a> SUSE Enterprise Linux Security Update for polkit (SUSE-SU-2022:0525-1)            |
| <a href="#">753642</a> SUSE Enterprise Linux Security Update for polkit (SUSE-SU-2022:0525-2)            |
| <a href="#">940483</a> AlmaLinux Security Update for polkit (ALSA-2022:1546)                             |

© [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](#)