



# CVE-2021-35938

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

## Summary

<b>CVE</b>	CVE-2021-35938
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-08-25 20:15:00 UTC
<b>Updated</b>	2022-11-29 18:06:00 UTC
<b>Description</b>	A symbolic link issue was found in rpm. It occurs when rpm sets the desired permissions and credentials after installing a fil

## Risk And Classification

**Problem Types:** CWE-59

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	8.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux</a>	9.0	All	All	All
Application	<a href="#">Rpm</a>	<a href="#">Rpm</a>	All	All	All	All

## References

Reference	Source	Link
Set file metadata via fd-based ops for everything but symlinks · rpm-software-management/rpm@25a435e · GitHub	MISC	<a href="#">github.</a>
rpm.org - Releases	MISC	<a href="#">rpm.or</a>
Bug 1157880 – VUL-0: CVE-2021-35938: rpm: races with chown/chmod/capabilities calls during installation	MISC	<a href="#">bugzill.</a>
Red Hat Customer Portal - Access to 24x7 support and knowledge	MISC	<a href="#">access</a>
1964114 – (CVE-2021-35938) CVE-2021-35938 rpm: races with chown/chmod/capabilities calls during installation	MISC	<a href="#">bugzill.</a>
RPM: Multiple Vulnerabilities (GLSA 202210-22) — Gentoo security	GENTOO	<a href="#">securit</a>
First steps towards fixing the symlink CVEs by pmatilai · Pull Request #1919 · rpm-software-management/rpm · GitHub	MISC	<a href="#">github.</a>
CVE Program record	CVE.ORG	<a href="#">www.c</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nis</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">161314</a> Oracle Enterprise Linux Security Update for rpm (ELSA-2024-0463)
<a href="#">161331</a> Oracle Enterprise Linux Security Update for rpm (ELSA-2024-0647)
<a href="#">182103</a> Debian Security Update for rpm (CVE-2021-35938)
<a href="#">242744</a> Red Hat Update for rpm (RHSA-2024:0424)
<a href="#">242754</a> Red Hat Update for rpm (RHSA-2024:0463)
<a href="#">242757</a> Red Hat Update for rpm (RHSA-2024:0435)
<a href="#">242810</a> Red Hat Update for rpm (RHSA-2024:0582)
<a href="#">242816</a> Red Hat Update for rpm (RHSA-2024:0647)
<a href="#">242842</a> Red Hat Update for rpm (RHSA-2024:0453)
<a href="#">357349</a> Amazon Linux Security Advisory for rpm : ALAS2023-2024-573
<a href="#">379634</a> Alibaba Cloud Linux Security Update for rpm (ALINUX3-SA-2024:0030)
<a href="#">502949</a> Alpine Linux Security Update for rpm
<a href="#">505818</a> Alpine Linux Security Update for rpm
<a href="#">672363</a> EulerOS Security Update for rpm (EulerOS-SA-2022-2741)
<a href="#">672374</a> EulerOS Security Update for rpm (EulerOS-SA-2022-2776)
<a href="#">672457</a> EulerOS Security Update for rpm (EulerOS-SA-2022-2829)
<a href="#">672471</a> EulerOS Security Update for rpm (EulerOS-SA-2022-2855)
<a href="#">691000</a> Free Berkeley Software Distribution (FreeBSD) Security Update for rpm4 (0c52abde-717b-11ed-98ca-40b034429ecf)
<a href="#">710651</a> Gentoo Linux RPM Multiple Vulnerabilities (GLSA 202210-22)
<a href="#">903712</a> Common Base Linux Mariner (CBL-Mariner) Security Update for rpm (10726)
<a href="#">903790</a> Common Base Linux Mariner (CBL-Mariner) Security Update for rpm (10723)
<a href="#">904163</a> Common Base Linux Mariner (CBL-Mariner) Security Update for rpm (10723-1)
<a href="#">941549</a> AlmaLinux Security Update for rpm (ALSA-2024:0463)
<a href="#">941568</a> AlmaLinux Security Update for rpm (ALSA-2024:0647)
<a href="#">961111</a> Rocky Linux Security Update for rpm (RLSA-2024:0647)

---

© [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](#)**