



# CVE-2021-3421

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

## Summary

<b>CVE</b>	CVE-2021-3421
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-05-19 14:15:00 UTC
<b>Updated</b>	2023-11-07 03:37:00 UTC
<b>Description</b>	A flaw was found in the RPM package in the read functionality. This flaw allows an attacker who can convince a victim to in:

## Risk And Classification

**Problem Types:** CWE-347

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
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>	6.0	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
Application	<a href="#">Rpm</a>	<a href="#">Rpm</a>	All	All	All	All
Application	<a href="#">Rpm</a>	<a href="#">Rpm</a>	All	All	All	All

## References

Reference	Source	L
[SECURITY] Fedora 34 Update: rpm-4.16.1.3-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lis</a>
[SECURITY] Fedora 34 Update: rpm-4.16.1.3-1.fc34 - package-announce - Fedora Mailing-Lists		<a href="#">lis</a>
[SECURITY] Fedora 33 Update: rpm-4.16.1.3-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lis</a>
[SECURITY] Fedora 33 Update: rpm-4.16.1.3-1.fc33 - package-announce - Fedora Mailing-Lists		<a href="#">lis</a>
[SECURITY] Fedora 32 Update: rpm-4.15.1.1-1.fc32.1 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="#">lis</a>
[SECURITY] Fedora 32 Update: rpm-4.15.1.1-1.fc32.1 - package-announce - Fedora Mailing-Lists		<a href="#">lis</a>

RPM: Multiple vulnerabilities (GLSA 202107-43) — Gentoo security	GENTOO	sc
1927747 – (CVE-2021-3421) CVE-2021-3421 rpm: unsigned signature header leads to string injection into an rpm database	MISC	bl
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

<a href="#">179989</a> Debian Security Update for rpm (CVE-2021-3421)
<a href="#">281435</a> Fedora Security Update for rpm (FEDORA-2021-662680e477)
<a href="#">281436</a> Fedora Security Update for rpm (FEDORA-2021-8d52a8a999)
<a href="#">281437</a> Fedora Security Update for rpm (FEDORA-2021-2383d950fd)
<a href="#">330113</a> IBM AIX Multiple Vulnerabilities due to RPM (rpm_advisory)
<a href="#">352470</a> Amazon Linux Security Advisory for rpm: ALAS-2021-1521
<a href="#">352485</a> Amazon Linux Security Advisory for rpm: ALAS2-2021-1689
<a href="#">501685</a> Alpine Linux Security Update for rpm
<a href="#">670407</a> EulerOS Security Update for rpm (EulerOS-SA-2021-1992)
<a href="#">670496</a> EulerOS Security Update for rpm (EulerOS-SA-2021-2254)
<a href="#">670522</a> EulerOS Security Update for rpm (EulerOS-SA-2021-2280)
<a href="#">670588</a> EulerOS Security Update for rpm (EulerOS-SA-2021-2346)
<a href="#">670685</a> EulerOS Security Update for rpm (EulerOS-SA-2021-2443)
<a href="#">671014</a> EulerOS Security Update for rpm (EulerOS-SA-2021-2613)
<a href="#">710026</a> Gentoo Linux RPM Multiple vulnerabilities (GLSA 202107-43)
<a href="#">750965</a> OpenSUSE Security Update for libdnf (openSUSE-SU-2021:2685-1)
<a href="#">750981</a> OpenSUSE Security Update for rpm (openSUSE-SU-2021:2682-1)
<a href="#">751248</a> OpenSUSE Security Update for rpm (openSUSE-SU-2021:1366-1)
<a href="#">752786</a> SUSE Enterprise Linux Security Update for rpm (SUSE-SU-2022:3939-1)
<a href="#">900173</a> CBL-Mariner Linux Security Update for rpm 4.14.2
<a href="#">903588</a> Common Base Linux Mariner (CBL-Mariner) Security Update for rpm (4268)
<a href="#">906239</a> Common Base Linux Mariner (CBL-Mariner) Security Update for rpm (4268-1)

© [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](#)**