



CVE-2021-3521

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

Summary

CVE	CVE-2021-3521
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-22 15:15:00 UTC
Updated	2023-02-12 23:41:00 UTC
Description	There is a flaw in RPM's signature functionality. OpenPGP subkeys are associated with a primary key via a "binding signature".

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rpm	Rpm	All	All	All	All

References

Reference

Red Hat Customer Portal - Access to 24x7 support and knowledge
1941098 – (CVE-2021-3521) CVE-2021-3521 rpm: RPM does not require subkeys to have a valid binding signature
Red Hat Customer Portal - Access to 24x7 support and knowledge
Validate and require subkey binding signatures on PGP public keys · rpm-software-management/rpm@bd36c5d · GitHub
Red Hat Customer Portal - Access to 24x7 support and knowledge
Red Hat Customer Portal - Access to 24x7 support and knowledge
RPM: Multiple Vulnerabilities (GLSA 202210-22) — Gentoo security
Validate and require subkey binding signatures on PGP public keys by pmatilai · Pull Request #1795 · rpm-software-management/rpm · GitHub
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159624 Oracle Enterprise Linux Security Update for rpm (ELSA-2022-0368)
183721 Debian Security Update for rpm (CVE-2021-3521)
240029 Red Hat Update for rpm (RHSA-2022:0254)
240052 Red Hat Update for rpm (RHSA-2022:0368)
240102 Red Hat Update for rpm (RHSA-2022:0634)
377369 Alibaba Cloud Linux Security Update for rpm (ALINUX3-SA-2022:0007)
502948 Alpine Linux Security Update for rpm
505817 Alpine Linux Security Update for rpm
671193 EulerOS Security Update for rpm (EulerOS-SA-2022-1015)
671227 EulerOS Security Update for rpm (EulerOS-SA-2022-1035)
671284 EulerOS Security Update for rpm (EulerOS-SA-2022-1234)
671300 EulerOS Security Update for rpm (EulerOS-SA-2022-1215)
672573 EulerOS Security Update for rpm (EulerOS-SA-2023-1335)
691000 Free Berkeley Software Distribution (FreeBSD) Security Update for rpm4 (0c52abde-717b-11ed-98ca-40b034429ecf)
710651 Gentoo Linux RPM Multiple Vulnerabilities (GLSA 202210-22)
903715 Common Base Linux Mariner (CBL-Mariner) Security Update for rpm (10647)
903827 Common Base Linux Mariner (CBL-Mariner) Security Update for rpm (10637)
904106 Common Base Linux Mariner (CBL-Mariner) Security Update for rpm (10647-1)
904138 Common Base Linux Mariner (CBL-Mariner) Security Update for rpm (10637-1)
940443 AlmaLinux Security Update for rpm (ALSA-2022:0368)
960109 Rocky Linux Security Update for rpm (RLSA-2022:368)
960692 Rocky Linux Security Update for rpm (RLSA-2022:0368)

© [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](#)