



CVE-2021-3445

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

Summary

CVE	CVE-2021-3445
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-19 14:15:00 UTC
Updated	2023-11-07 03:38:00 UTC
Description	A flaw was found in libdnf's signature verification functionality in versions before 0.60.1. This flaw allows an attacker to achieve

Risk And Classification

Problem Types: CWE-347

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Redhat	Enterprise Linux	8.0	All	All	All
Application	Rpm	Libdnf	All	All	All	All

References

Reference

- [SECURITY] Fedora 33 Update: rpm-ostree-2021.4-1.fc33 - package-announce - Fedora Mailing-Lists
- [SECURITY] Fedora 34 Update: rpm-ostree-2021.4-1.fc34 - package-announce - Fedora Mailing-Lists
- [SECURITY] Fedora 33 Update: rpm-ostree-2021.4-1.fc33 - package-announce - Fedora Mailing-Lists
- 1932079 – (CVE-2021-3445) CVE-2021-3445 libdnf: libdnf does its own signature verification, but this can be tricked by placing a signature in
- [SECURITY] Fedora 34 Update: rpm-ostree-2021.4-1.fc34 - package-announce - Fedora Mailing-Lists
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

159517 Oracle Enterprise Linux Security Update for dnf (ELSA-2021-4464)
179923 Debian Security Update for libdnf (CVE-2021-3445)
239847 Red Hat Update for dnf (RHSA-2021:4464)
281318 Fedora Security Update for rpm (FEDORA-2021-eadfc56b95)
281319 Fedora Security Update for rpm (FEDORA-2021-c6802f0b69)
670710 EulerOS Security Update for libdnf (EulerOS-SA-2021-2468)
670773 EulerOS Security Update for libdnf (EulerOS-SA-2021-2531)
670797 EulerOS Security Update for libdnf (EulerOS-SA-2021-2555)
670934 EulerOS Security Update for libdnf (EulerOS-SA-2021-2468)
750965 OpenSUSE Security Update for libdnf (openSUSE-SU-2021:2685-1)
900043 CBL-Mariner Linux Security Update for libdnf 0.43.1
902828 Common Base Linux Mariner (CBL-Mariner) Security Update for libdnf (4245)
940302 AlmaLinux Security Update for dnf (ALSA-2021:4464)
960804 Rocky Linux Security Update for dnf (RLSA-2021:4464)

© [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](#)