



CVE-2017-7500

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

Summary

CVE	CVE-2017-7500
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-13 17:29:00 UTC
Updated	2019-10-09 23:29:00 UTC
Description	It was found that rpm did not properly handle RPM installations when a destination path was a symbolic link to a directory, p

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rpm	Rpm	All	All	All	All
Application	Rpm	Rpm	4.14.0.0	rc1	All	All
Application	Rpm	Rpm	4.14.0.0	rc2	All	All
Application	Rpm	Rpm	All	All	All	All
Application	Rpm	Rpm	4.14.0.0	rc1	All	All
Application	Rpm	Rpm	4.14.0.0	rc2	All	All

References

Reference	Score
Restrict following symlinks to directories by ownership (CVE-2017-7500) · rpm-software-management/rpm@f2d3be2 · GitHub	CC
Make verification match the new restricted directory symlink behavior · rpm-software-management/rpm@c815822 · GitHub	CC
1450369 – (CVE-2017-7500) CVE-2017-7500 rpm: Following symlinks to directories when installing packages allows privilege escalation	CC
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

671076 EulerOS Security Update for rpm (EulerOS-SA-2019-2658)

© [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](#)