



CVE-2023-2319

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2023-2319
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-17 23:15:00 UTC
Updated	2023-05-26 13:33:00 UTC
Description	It was discovered that an update for PCS package in RHBA-2023:2151 erratum released as part of Red Hat Enterprise Linux

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Clusterlabs	Pcs	0.11.4-6.el9	All	All	All
Operating System	Redhat	Enterprise Linux High Availability	9.0	All	All	All
Operating System	Redhat	Enterprise Linux High Availability Eus	9.2	All	All	All

References

Reference	Source
cve-details	MISC
Red Hat	MISC
2190092 – (CVE-2023-2319) CVE-2023-2319 pcs: webpack: Regression of CVE-2023-28154 fixes in the Red Hat Enterprise Linux	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160798](#) Oracle Enterprise Linux Security Update for pcs (ELSA-2023-12595)

[241425](#) Red Hat Update for pcs (RHSA-2023:2652)

941058 AlmaLinux Security Update for pcs (ALSA-2023:2652)

960940 Rocky Linux Security Update for pcs (RLSA-2023:2652)

© [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](#)