



CVE-2024-26141

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

Summary

CVE	CVE-2024-26141
State	PUBLISHED
Assigner	Unknown
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-02-29 00:15:00 UTC
Updated	2024-02-29 13:49:00 UTC
Description	Description unavailable.

There are no known software configurations currently associated with this CVE in NVD or the CVE Program record.

References

Reference	Source	Link
github.com/rack/rack/security/advisories/GHSA-xj5v-6v4g-jfw6		github.com
github.com/rubysec/ruby-advisory-db/blob/master/gems/rack/CVE-2024-26141...		github.com
Possible DoS Vulnerability with Range Header in Rack - Security Announcements - Ruby on Rails Discussions		discuss.rubyonrails.org
Return an empty array when ranges are too large · rack/rack@6245768 · GitHub		github.com
github.com/rack/rack/commit/4849132bef471adb21131980df745f4bb84de2d9		github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

200188 Ubuntu Security Notification for Rack Vulnerabilities (USN-6689-1)
357336 Amazon Linux Security Advisory for pcs : ALAS2-2024-2492
755907 SUSE Enterprise Linux Security Update for rubygem-rack (SUSE-SU-2024:0765-1)
997568 Rubygems (Rubygems) Security Update for rack (GHSA-xj5v-6v4g-jfw6)

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](#)