CVE-2022-23633

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-23633
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-11 21:15:00 UTC
Updated	2024-01-19 16:15:00 UTC
Description	Action Pack is a framework for handling and responding to web requests. Under certain circumstances response bodies wil

Risk And Classification

Problem Types: CWE-212

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Rubyonrails	Rails	All	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 3093-1] rails security update	MLIST	lists.debian.org	
oss-security - [CVE-2022-23633] Possible exposure of information vulnerability in Action Pack	MLIST	www.openwall.com	
Possible exposure of information vulnerability in Action Pack · Advisory · rails/rails · GitHub	CONFIRM	github.com	
Debian -- Security Information -- DSA-5372-1 rails	DEBIAN	www.debian.org	
CVE-2022-23633 Ruby on Rails Vulnerability in NetApp Products | NetApp Product Security		security.netapp.com	
Fix reloader to work with new Executor signature · rails/rails@f9a2ad0 · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

180989 Debian Security Update for rails (DLA 3093-1)

181676 Debian Security Update for rails (DSA 5372-1)

184142 Debian Security Update for rails (CVE-2022-23633)

240566 Red Hat Update for Satellite 6.11 Release (RHSA-2022:5498)

753313 SUSE Enterprise Linux Security Update for rubygem-actionpack-5_1, rubygem-activesupport-5_1 (SUSE-SU-2022:2108-1)

960505 Rocky Linux Security Update for Satellite (RLSA-2022:5498)

© 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 registred 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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**