



CVE-2021-22942

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

Summary

CVE	CVE-2021-22942
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-18 13:15:00 UTC
Updated	2024-02-02 14:15:00 UTC
Description	A possible open redirect vulnerability in the Host Authorization middleware in Action Pack >= 6.0.0 that could allow attacker

Risk And Classification

Problem Types: CWE-601

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rubyonrails	Rails	All	All	All	All

References

Reference	Source	Link	Tags
CVE-2021-22942 Ruby on Rails Vulnerability in NetApp Products NetApp Product Security		security.netapp.com	
Debian -- Security Information -- DSA-5372-1 rails	DEBIAN	www.debian.org	
oss-security - [CVE-2021-44528] Possible Open Redirect in Host Authorization Middleware	MLIST	www.openwall.com	
Rails 6.0.4.1 and 6.1.4.1 have been released Riding Rails	MISC	weblog.rubyonrails.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

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

[183947](#) Debian Security Update for rails (CVE-2021-22942)

© [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](#)