



CVE-2020-8159

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

Summary

CVE	CVE-2020-8159
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-12 13:15:00 UTC
Updated	2023-11-07 03:26:00 UTC
Description	There is a vulnerability in actionpack_page-caching gem < v1.2.1 that allows an attacker to write arbitrary files to a web ser

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Rubyonrails	Actionpack Page-caching	All	All	All	All
Application	Rubyonrails	Actionpack Page-caching	All	All	All	All

References

Reference	Source	Link	Tags
Google Groups		groups.google.com	
[SECURITY] [DLA 2719-1] ruby-actionpack-page-caching security update	MLIST	lists.debian.org	
Google Groups	MISC	groups.google.com	Exploit, Mailing List, Patch, Th
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[178722](#) Debian Security Update for ruby-actionpack-page-caching (DLA 2719-1)

© [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](#)