

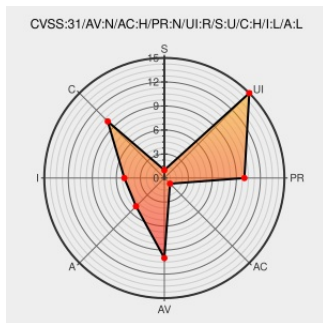


CVE-2020-11082

Published on: 05/28/2020 12:00:00 AM UTC

Last Modified on: 11/30/2021 10:07:00 PM UTC

CVE-2020-11082 - advisory for GHSA-r5jw-62xg-j433

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

In Kaminari before 1.2.1, there is a vulnerability that would allow an attacker to inject arbitrary code into pages with pagination links. This has been fixed in 1.2.1.

CVE-2020-11082 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: kaminari - Kaminari version < 1.2.1

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
	Broken Link github.com	MISC github.com/github/advisory-review/pull/1020

	github.com text/plain Inactive Link Not Archived	
Debian -- Security Information -- DSA-5005-1 ruby-kaminari	www.debian.org Deprecated Link text/html	DEBIAN DSA-5005
[SECURITY] [DLA 2763-1] ruby-kaminari security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20210922 [SECURITY] [DLA 2763-1] ruby-kaminari security update
Blacklist "original_script_name" get param · kaminari/kaminari@8dd52a1 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/kaminari/kaminari/commit/8dd52a1aed3d2fa2835d836de23fc0d8c4ff5c
Potential Cross Site Scripting · Advisory · kaminari/kaminari · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/kaminari/kaminari/security/advisories/GHSA-r5jw-62xg-j

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

- 178804 Debian Security Update for ruby-kaminari (DLA 2763-1)
- 178888 Debian Security Update for ruby-kaminari (DSA 5005-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Kaminari Project	Kaminari	All	All	All	All
Application	Kaminari Project	Kaminari	All	All	All	All
cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:a:kaminari_project:kaminari:*:*:*:*:*:						
cpe:2.3:a:kaminari_project:kaminari:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

[← Previous ID](#)[Next ID →](#)

© [CVE.report](#) 2023  |

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](#)