

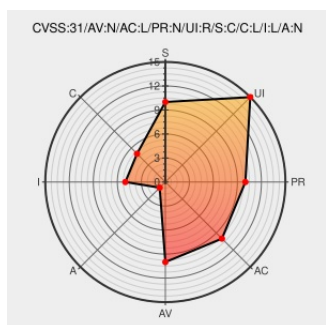


CVE-2023-30614

Published on: Not Yet Published

Last Modified on: 05/15/2023 07:27:00 PM UTC

CVE-2023-30614 - advisory for GHSA-cqf3-vpx7-rxhw

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

Certain versions of [Pay](#) from [Pay Project](#) contain the following vulnerability:

Pay is a payments engine for Ruby on Rails 6.0 and higher. In versions prior to 6.3.2 a payments info page of Pay is susceptible to reflected Cross-site scripting. An attacker could create a working URL that renders a javascript link to a user on a Rails application that integrates Pay. This URL could be distributed via email to specifically target

certain individuals. If the targeted application contains a functionality to submit user-generated content (such as comments) the attacker could even distribute the URL using that functionality. This has been patched in version 6.3.2 and above. Users are advised to upgrade. There are no known workarounds for this vulnerability.

CVE-2023-30614 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [pay-rails](#) - **pay** version = < 6.3.2

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

CVE References

Description	Tags	Link
Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) in pay · Advisory · pay-rails/pay · GitHub	github.com text/html	MISC github.com/pay-rails/pay/security/advisories/GHSA-cqf3-vpx7-rxhw
Fix XSS vulnerability on Stripe payment page · pay-rails/pay@5d6283a · GitHub	github.com text/html	MISC github.com/pay-rails/pay/commit/5d6283a24062bd272a524ac48415f536a67ad57f

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pay Project	Pay	All	All	All	All
Application	Pay Project	Pay	All	All	All	All
cpe:2.3:a:pay_project:pay:*:*:*:*:rails:*:*:						
cpe:2.3:a:pay_project:pay:*:*:*:*:ruby:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2023-30614 : Pay is a payments engine for Ruby on Rails 6.0 and higher. In versions prior to 6.3.2 a payments i... twitter.com/i/web/status/1...	2023-04-19 18:05:17

[← 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