



CVE-2021-29481

Published on: 06/29/2021 12:00:00 AM UTC

Last Modified on: 07/07/2021 04:44:00 PM UTC

CVE-2021-29481 - advisory for GHSA-phj8-4cq3-794g

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

CVSS:31/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N



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

Ratpack is a toolkit for creating web applications. In versions prior to 1.9.0, the default configuration of client side sessions results in unencrypted, but signed, data being set as cookie values. This means that if something sensitive goes into the session, it could be read by something with access to the cookies. For this to be a vulnerability,

some kind of sensitive data would need to be stored in the session and the session cookie would have to leak. For example, the cookies are not configured with httpOnly and an adjacent XSS vulnerability within the site allowed capture of the cookies. As of version 1.9.0, a securely randomly generated signing key is used. As a workaround, one may supply an encryption key, as per the documentation recommendation.

CVE-2021-29481 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [ratpack](#) - **ratpack** version < 1.9.0

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

PARTIAL

NONE

NONE

CVE References

Description	Tags	Link
Use random UUID for default client side session encryption secret by Idaley · Pull Request #1590 · ratpack/ratpack · GitHub	github.com text/html	 MISC github.com/ratpack/ratpack/pull/1590
Client side sessions should not allow unencrypted storage · Advisory · ratpack/ratpack · GitHub	github.com text/html	 CONFIRM github.com/ratpack/ratpack/security/advisories/GHSA-phj8-4cq3-794g

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

981302 Java (maven) Security Update for io.ratpack:ratpack-session (GHSA-phj8-4cq3-794g)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ratpack Project	Ratpack	All	All	All	All
cpe:2.3:a:ratpack_project:ratpack:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-29481 : Ratpack is a toolkit for creating web applications. In versions prior to 1.9.0, the default config... twitter.com/i/web/status/1...	2021-06-29 18:24:40
 /r/netcve	CVE-2021-29481	2021-06-29 18:41:43

[← 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](#)