

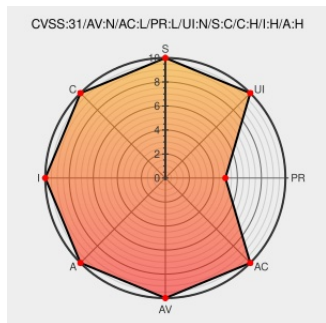


CVE-2021-29485

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

Last Modified on: 07/08/2021 03:26:00 PM UTC

CVE-2021-29485 - advisory for GHSA-hc33-32vw-rpp9

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

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, a malicious attacker can achieve Remote Code Execution (RCE) via a maliciously crafted Java deserialization gadget chain leveraged against the Ratpack session store. If one's application does not use Ratpack's session mechanism, it is not vulnerable. Ratpack 1.9.0

introduces a strict allow-list mechanism that mitigates this vulnerability when used. Two possible workarounds exist. The simplest mitigation for users of earlier versions is to reduce the likelihood of attackers being able to write to the session data store. Alternatively or additionally, the allow-list mechanism could be manually back ported by providing an alternative implementation of `SessionSerializer` that uses an allow-list.

CVE-2021-29485 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: **8.8 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact

CVE References

Description	Tags	Link
Maven Repository: io.ratpack » ratpack-core	web.archive.org text/html Inactive Link Not Archived	 MISC mvnrepository.com/artifact/io.ratpack/ratpack-core
Remote Code Execution Vulnerability in Session Storage · Advisory · ratpack/ratpack · GitHub	github.com text/html	 CONFIRM github.com/ratpack/ratpack/security/advisories/GHSA-hc33-32vw-rpp9

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

980386 Java (maven) Security Update for io.ratpack:ratpack-core (GHSA-hc33-32vw-rpp9)

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-2021-29485 : Ratpack is a toolkit for creating web applications. In versions prior to 1.9.0, a malicious attack... twitter.com/i/web/status/1...	2021-06-29 18:38:19
 /r/netcve	CVE-2021-29485	2021-06-29 19:41:45

[← 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](#)