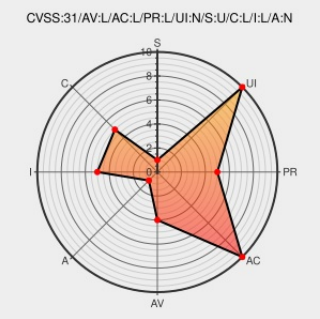
CVE-2021-29480

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

Last Modified on: 08/02/2022 04:00:00 PM UTC

CVE-2021-29480 - advisory for GHSA-2cc5-23r7-vc4v

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, the client side session module uses the application startup time as the signing key by default. This means that if an attacker can determine this time, and if encryption is not also used (which is recommended, but is not on by default), the session data could be tampered with by someone with the ability to write cookies. The default configuration is unsuitable for production use as an application restart renders all sessions invalid and is not multi-host compatible, but its use is not actively prevented. As of Ratpack 1.9.0, the default value is a securely randomly generated value, generated at application startup time. As a workaround, supply an alternative signing key, as per the documentation's recommendation.

CVE-2021-29480 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as LOW severity.

Affected Vendor/Software: **ratpack** - **ratpack** version **< 1.9.0**

CVSS3 Score: 3.1 - LOW

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

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

NONE | PARTIAL | NONE

CVE References

Description	Tags	Link
Default client side session signing key is highly predictable · Advisory · ratpack/ratpack · GitHub	github.com text/html	CONFIRM github.com/ratpack/ratpack/security/advisories/GHSA-2cc5-23
ratpack/ClientSideSessionConfig.java at 29434f7ac6fd4b36a4495429b70f4c8163100332 · ratpack/ratpack · GitHub	github.com text/html	MISC github.com/ratpack/ratpack/blob/29434f7ac6fd4b36a4495429b70f4c8163100 session/src/main/java/ratpack/session/clientside/ClientSideSessionConfig.jav

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

982013 Java (maven) Security Update for io.ratpack:ratpack-session (GHSA-2cc5-23r7-vc4v)

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-2021-29480 : Ratpack is a toolkit for creating web applications. In versions prior to 1.9.0, the client side se… twitter.com/i/web/status/1…	2021-06-29 18:17:37
/r/netcve	CVE-2021-29480	2021-06-29 18:41:42

← Previous ID | Next ID→

CVE.report and Source URL Uptime Status status.cve.report