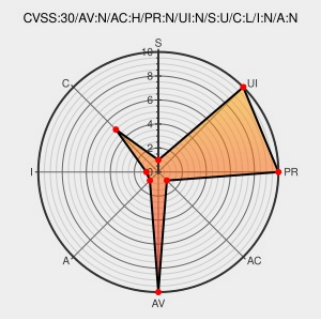
CVE-2019-11808

Published on: 05/07/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:35 PM UTC

CVE-2019-11808

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ratpack from Ratpack Project contain the following vulnerability:

Ratpack versions before 1.6.1 generate a session ID using a cryptographically weak PRNG in the JDK's ThreadLocalRandom. This means that if an attacker can determine a small window for the server start time and obtain a session ID value, they can theoretically determine the sequence of session IDs.

CVE-2019-11808 has been assigned by cve@mitre.org to track the vulnerability - currently rated as LOW severity.

CVSS3 Score: 3.7 - LOW

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Release v1.6.1 · ratpack/ratpack · GitHub	Release Notes, Third Party Advisory, github.com	MISC github.com/ratpack/ratpack/releases/tag/v1.6.1

	text/html	
Use UUID directly for generating session IDs · ratpack/ratpack@f2b63eb · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/ratpack/ratpack/commit/f2b63eb82dd71194319fd3945f5edf29b8f3a42d
Use UUID directly for generating session IDs · Issue #1448 · ratpack/ratpack · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/ratpack/ratpack/issues/1448

Related QID Numbers

981788 Java (maven) Security Update for io.ratpack:ratpack-groovy (GHSA-54mg-vgrp-mwx9)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ratpack Project	Ratpack	All	All	All	All
Application	Ratpack Project	Ratpack	All	All	All	All

cpe:2.3:a:ratpack_project:ratpack:*:*:*:*:*:*:*:*:

cpe:2.3:a:ratpack_project:ratpack:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→