# CVE Detail – CVE-2022-39218

The JS Compute Runtime for Fastly's Compute@Edge platform provides the environment JavaScript is executed in when using the Compute@Edge JavaScript SDK. In versions prior to 0.5.3, the `Math.random` and `crypto.getRandomValues` methods fail to use sufficiently random values. The initial value to seed the PRNG (pseudorandom number generator) is baked-in to the final WebAssembly module, making the sequence of random values for that specific WebAssembly module predictable. An attacker can use the fixed seed to predict random numbers generated by these functions and bypass cryptographic security controls, for example to disclose sensitive data encrypted by functions that use these generators. The problem has been patched in version 0.5.3. No known workarounds exist.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.32928

## CVSS Scoring

CVSS v3.1 Score: 7.5

Severity: HIGH

## Mapped CWE(s)

* CWE-335: Incorrect Usage of Seeds in Pseudo-Random Number Generator (PRNG)

## Affected Products

* cpe:2.3:a:fastly:js-compute:\*:\*:\*:\*:\*:node.js:\*:\*