Unauthorized takeover for new versions of some platform-specific gems

Critical **indirect** published **GHSA-2jmx-8mh8-pm8w** on May 11

Package

rubygems.org (RubyGems)

Affected versions	Patched versions
n/a	n/a

Description

Summary

An ordering mistake in the code that accepts gem uploads allowed some gems (with platforms ending in numbers, like `arm64-darwin-21`) to be temporarily replaced in the CDN cache by a malicious package.

The bug has been patched, and we believe it was never exploited, based on an extensive review of our logs and existing gems.

Impact

No known impact. The issue was patched in production within 4 hours of the report to Hacker One, and the exploit generates a distinctive exception report that does not appear in our logs prior to today.

The `nokogiri` gem was determined to not be vulnerable to this issue within the last two years, due to all releases since February 2020 using platforms without numbers (like `arm64-darwin`).

In our analysis, the only gems that could have been exploited this way in the last 6 months are `libv8-node` and `sorbet-static`. We found no evidence of such an exploit when reviewing those gems.

Verification

The easiest way to ensure that your applications were not exploited by this vulnerability is to check that all of your downloaded .gems have a checksum that matches the checksum recorded in the RubyGems.org database.

RubyGems contributor Maciej Mensfeld wrote a tool to automatically check that all downloaded .gem files match the checksums recorded in the RubyGems.org database. You can use it by running:

```
bundle add bundler-integrity
bundle exec bundler-integrity
```

Neither this tool nor anything else can prove you were not exploited, but the can assist your investigation by quickly comparing RubyGems API-provided checksums with the checksums of files on your disk.

Details

This vulnerability was limited to platform-specific gems ending in a number, for example `sorbet-static`, version `0.5.9995`, platform `universal-darwin-20`.

1. An attacker could guess the next version number, and create a gem with the name `sorbet-static-0.5.9996-universal-darwin` and version number `20`.
2. With a crafted invalid gemspec, it was possible to coerce RubyGems.org to save that gem to S3 without creating a matching database record.
3. Later, the real `sorbet-static` gem would release version `0.5.9996` as usual, and the attacker-controlled file would be overwritten on S3.
4. However, if the attacker had already primed the Fastly CDN cache by requesting their malicious gem, Fastly would continue to serve the old, malicious package.

We resolved this issue by patching the logic bug to ensure files are not written to S3 until the end of the database transaction, and we now purge the Fastly cache any time a gem is written to S3. After deploying and verifying the fix, we purged the entire Fastly cache to guarantee no malicious gems could remain present.

Severity

Critical

CVE ID

CVE-2022-29218

Weaknesses

No CWEs

Credits

 laursisask