[CVE-2020-8166] Ability to forge per-form CSRF tokens given a global CSRF token

Aaron Patterson

to rubyonrail...@googlegroups.com, ruby-sec...@googlegroups.com

Ability to forge per-form CSRF tokens given a global CSRF token

It is possible to possible to, given a global CSRF token such as the one present in the authenticity_token meta tag, forge a per-form CSRF token for any action for that session. This vulnerability has been assigned the CVE identifier CVE-2020-8166.

Versions Affected: rails < 5.2.5, rails < 6.0.4
Not affected: Applications without existing HTML injection vulnerabilities.
Fixed Versions: rails >= 5.2.4.3, rails >= 6.0.3.1

Impact

Given the ability to extract the global CSRF token, an attacker would be able to construct a per-form CSRF token for that session.

Releases

The fixed releases are available on RubyGems.

Workarounds

This is a low-severity security issue. As such, no workaround is necessarily until such time as the application can be upgraded.

Patches

For developers who are not able to immediately patch their applications, we are including the following patches for Rails 6.0.3 and Rails 5.2.4.2.

* 5-2-per-form-csrf.patch - Patch for 5.2 series
* 6-0-per-form-csrf.patch - Patch for 6.0 series

Credits

Thanks to https://hackerone.com/jregele for reporting this issue via our HackerOne bug bounty program.

5-2-per-form-csr...

6-0-per-form-csr...

Reply all Reply to author Forward