[CVE-2020-8159] Arbitrary file write/potential remote code execution in actionpack_page-caching

1241 views

Aaron Patterson May 6, 2020, 12:46:34 PM

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

Arbitrary file write/potential remote code execution in actionpack_page-caching

There is a vulnerability in the actionpack_page-caching gem that allows an attacker to write arbitrary files to a web server, potentially resulting in remote code execution if the attacker can write unescaped ERB to a view.

This vulnerability has been assigned the CVE identifier CVE-2020-8159.

Versions Affected: All versions of actionpack_page-caching (part of Rails prior to Rails 4.0)
Not affected: Applications not using actionpack_page-caching
Fixed Versions: actionpack_page-caching >= 1.2.1

Impact

The Action Pack Page Caching gem writes cache files to the file system in order for the front end webserver (nginx, Apache, etc) to serve the cached file without making a request to the application server. Paths contain what