Security advisories: CVE-2025-27219, CVE-2025-27220 and CVE-2025-27221

Posted by **hsbt** on 26 Feb 2025

We published security advisories for CVE-2025-27219, CVE-2025-27220 and CVE-2025-27221. Please read the details below.

CVE-2025-27219: Denial of Service in `CGI::Cookie.parse`.

There is a possibility for DoS by in the cgi gem. This vulnerability has been assigned the CVE identifier CVE-2025-27219 (https://www.cve.org/CVERecord?id=CVE-2025-27219). We recommend upgrading the cgi gem.

Details

`CGI::Cookie.parse` took super-linear time to parse a cookie string in some cases. Feeding a maliciously crafted cookie string into the method could lead to a Denial of Service.

Please update CGI gem to version 0.3.5.1, 0.3.7, 0.4.2 or later.

Affected versions

- cgi gem versions <= 0.3.5, 0.3.6, 0.4.0 and 0.4.1.

Credits

Thanks to lio346 (https://hackerone.com/lio346) for discovering this issue. Also thanks to mame (https://github.com/mame) for fixing this vulnerability.

CVE-2025-27220: ReDoS in `CGI::Util#escapeElement`.

There is a possibility for Regular expression Denial of Service(ReDoS) by in the cgi gem. This vulnerability has been assigned the CVE identifier CVE-2025-27220 (https://www.cve.org/CVERecord?id=CVE-2025-27220). We recommend upgrading the cgi gem.

Details

The regular expression used in `CGI::Util#escapeElement` is vulnerable to ReDoS. The crafted input could lead to a high CPU consumption.

This vulnerability only affects Ruby 3.1 and 3.2. If you are using these versions, please update CGI gem to version 0.3.5.1, 0.3.7, 0.4.2 or later.

Affected versions

- cgi gem versions <= 0.3.5, 0.3.6, 0.4.0 and 0.4.1.

Credits

Thanks to svalkanov (https://hackerone.com/svalkanov) for discovering this issue. Also thanks to nobu (https://github.com/nobu) for fixing this vulnerability.

CVE-2025-27221: userinfo leakage in `URI#join`, `URI#merge` and `URI#+`.

There is a possibility for userinfo leakage by in the uri gem. This vulnerability has been assigned the CVE identifier CVE-2025-27221 (https://www.cve.org/CVERecord?id=CVE-2025-27221). We recommend upgrading the uri gem.

Details

The methods `URI#join`, `URI#merge`, and `URI#+` retained userinfo, such as `user:password`, even after the host is replaced. When generating a URL to a malicious host from a URL containing secret userinfo using these methods, and having someone access that URL, an unintended userinfo leak could occur.

Please update URI gem to version 0.11.3, 0.12.4, 0.13.2, 1.0.3 or later.

Affected versions

- uri gem versions < 0.11.3, 0.12.0 to 0.12.3, 0.13.0, 0.13.1 and 1.0.0 to 1.0.2.

Credits

Thanks to Tsubasa Irisawa (lambdasawa) (https://hackerone.com/lambdasawa) for discovering this issue. Also thanks to nobu (https://github.com/nobu) for additional fixes of this vulnerability.

History

- Originally published at 2025-02-26 7:00:00 (UTC)

Recent News >

Ruby 4.0.3 Released

Ruby 4.0.3 has been released.

Posted by **k0kubun** on 21 Apr 2026

Ruby 3.2.11 Released

Ruby 3.2.11 has been released. This release includes an update to the zlib gem addressing CVE-2026-27820.

Posted by **hsbt** on 27 Mar 2026

Ruby 3.3.11 Released

Ruby 3.3.11 has been released. This release includes an update to the zlib gem addressing CVE-2026-27820, along with some bug fixes.

Posted by **hsbt** on 26 Mar 2026

Ruby 4.0.2 Released

Ruby 4.0.2 has been released.

Posted by **k0kubun** on 16 Mar 2026

More News... >