GitHub Advisory Database / GitHub Reviewed / CVE-2025-27221

URI allows for userinfo Leakage in URI#join, URI#merge, and URI#+

Low severity | GitHub Reviewed | Published on Mar 3, 2025 to the GitHub Advisory Database • Updated on Nov 4, 2025

Vulnerability details | Dependabot alerts 0

Package

uri (RubyGems)

Affected versions	Patched versions
< 0.11.3	0.11.3
>= 0.12.0, < 0.12.4	0.12.4
>= 0.13.0, < 0.13.2	0.13.2
>= 1.0.0, < 1.0.3	1.0.3

Description

There is a possibility for userinfo leakage by in the uri gem.
This vulnerability has been assigned the CVE identifier 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) for discovering this issue.
Also thanks to nobu for additional fixes of this vulnerability.

References

- ruby/uri#154
- ruby/uri#155
- ruby/uri#156
- ruby/uri#157
- https://github.com/rubysec/ruby-advisory-db/blob/master/gems/uri/CVE-2025-27221.yml
- https://www.cve.org/CVERecord?id=CVE-2025-27221
- https://www.ruby-lang.org/en/news/2025/02/26/security-advisories
- https://nvd.nist.gov/vuln/detail/CVE-2025-27221
- https://hackerone.com/reports/2957667
- https://lists.debian.org/debian-lts-announce/2025/05/msg00015.html
- https://lists.debian.org/debian-lts-announce/2025/03/msg00008.html

Published to the GitHub Advisory Database on Mar 3, 2025

Reviewed on Mar 3, 2025

Published by the National Vulnerability Database on Mar 4, 2025

Last updated on Nov 4, 2025

Severity

Low 2.1 / 10

CVSS v4 base metrics

Exploitability Metrics

Attack Vector	Local
Attack Complexity	Low
Attack Requirements	Present
Privileges Required	None
User interaction	None

Vulnerable System Impact Metrics

Confidentiality	None
Integrity	None
Availability	None
Subsequent System Impact Metrics	
Confidentiality	Low
Integrity	None
Availability	None

Learn more about base metrics

CVSS:4.0/AV:L/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N

EPSS score

0.137% (34th percentile)

Weaknesses

- CWE-200
- CWE-212

CVE ID

CVE-2025-27221

GHSA ID

GHSA-22h5-pq3x-2gf2

Source code

ruby/uri

Credits

john-halderman Analyst

This advisory has been edited. See History.

See something to contribute? Suggest improvements for this vulnerability.