URI Credential Leakage Bypass over CVE-2025-27221

High **hsbt** published **GHSA-j4pr-3wm6-xx2r** 2 weeks ago

Package

uri (RubyGems)

Affected versions

<= 0.12.4, <= 0.13.2, <= 1.0.3

Patched versions

0.12.5, 0.13.3, 1.0.4

Description

Impact

In affected URI version, a bypass exists for the fix to CVE-2025-27221 that can expose user credentials.

When using the `+` operator to combine URIs, sensitive information like passwords from the original URI can be leaked, violating RFC3986 and making applications vulnerable to credential exposure.

The vulnerability affects the `uri` gem bundled with the following Ruby series:

- 0.12.4 and earlier (bundled in Ruby 3.2 series)
- 0.13.2 and earlier (bundled in Ruby 3.3 series)
- 1.0.3 and earlier (bundled in Ruby 3.4 series)

Patches

Upgrade to 0.12.5, 0.13.3 or 1.0.4

References

- https://www.ruby-lang.org/en/news/2025/02/26/security-advisories/
- https://hackerone.com/reports/2957667

Severity

High

CVE ID

CVE-2025-61594

Weaknesses

No CWEs