

Regexp compilation fixes related to GitLab's CVE-2026-89078, CVE-2026-93577, CVE-2026-97229 and CVE-2026-110264

Posted by **k0kubun** on 23 Oct 2026

We have released Ruby 4.0.9, 3.4.12 and 3.3.13. They fix several bugs in Ruby's regular expression engine (Onigmo) that GitLab found could be used for remote code execution on GitLab servers. GitLab published four CVEs for these issues, and the Ruby releases contain the fixes for the underlying bugs in Ruby.

Background

GitLab compiles regular expressions supplied by its users, such as patterns in CI configuration, with `Regexp.new`. GitLab found that specially crafted patterns could corrupt memory while Ruby compiles them, and that this could be turned into remote code execution on GitLab servers. GitLab addressed these issues in its own releases by patching the Ruby it ships, and assigned the following CVE identifiers:

- [CVE-2026-89078](#): Double Free issue in Regular Expression Parser ([GitLab 19.4.1](#))
- [CVE-2026-93577](#): Integer Overflow issue in Regular Expression Compiler ([GitLab 19.4.1](#))
- [CVE-2026-97229](#): Integer Overflow issue in CI/CD Regular Expression Compiler ([GitLab 19.4.2](#))
- [CVE-2026-110264](#): Integer Overflow issue in Regular Expression Compiler ([GitLab 19.5.1](#))

Fixes in Ruby

The following table shows the change in Ruby that fixes the bug behind each CVE, and the first release of each series that contains it.

GitLab CVE	Bug in Ruby	Change	Ruby 4.0	Ruby 3.4	Ruby 3.3
CVE-2026-89078	Double free when parsing a pattern fails after an alternation	#13332	4.0.0	3.4.12	3.3.13
CVE-2026-93577, CVE-2026-97229	Integer overflow in the size of a compiled pattern	#19020	4.0.8	3.4.12	3.3.13
CVE-2026-110264	Overflow of internal IDs in a pattern with many repeats	#16801	4.0.9	3.4.12	3.3.13

Ruby 4.0.9, 3.4.12 and 3.3.13 contain all of these fixes.

Who is affected

These bugs are reached only when an application compiles a regular expression from a string that an attacker controls, for example by passing it to `Regexp.new`, `Regexp.union` or `Regexp.compile`, or by interpolating it into a regexp literal such as `/#{input}/`. Applications that only use regular expressions written by their own developers are not affected.

`Regexp.timeout` does not protect against these bugs. Limiting the length of patterns does not reliably protect against them either, because some of them can be triggered by short patterns.

Recommended action

We recommend upgrading to Ruby 4.0.9, 3.4.12 or 3.3.13 or later.

If you cannot upgrade, please avoid compiling regular expressions from untrusted input.

Ruby 3.3 is in the security maintenance phase, in which we normally release only fixes for vulnerabilities. Ruby 3.3.13 includes these fixes as an exception, because GitLab assigned CVEs to issues that rely on them.

About CVE identifiers

We have not requested CVE identifiers in Ruby for these fixes, at least for now.

Ruby has generally considered it unsafe to compile and use a regular expression created from untrusted input. We stated this in the advisory for [CVE-2022-28738](#), where we nevertheless treated a double free in Regexp compilation as a vulnerability after a comprehensive assessment. We did the same for [CVE-2024-27282](#).

However, the [Regexp documentation](#) currently discusses untrusted patterns only in terms of denial of service, and recommends a timeout for them. It does not clearly say whether compiling an untrusted pattern is a use case that Ruby supports. We plan to discuss how to document this, and whether we treat this kind of issue as a vulnerability in Ruby, including whether to request CVE identifiers for these fixes. If we request any, we will update this page.

In the meantime, please refer to GitLab's CVE identifiers listed above when you track these issues, for example in a security scanner.

Credits

Thanks to Johan Carlsson ([joaxcar](#)) for discovering the integer overflow fixed by [#19020](#) through GitLab's bug bounty program, and to GitLab for reporting these issues to us and coordinating the fixes.

History

- Originally published at 2026-10-23 03:11:22 (UTC)

Recent News

Ruby 3.3.13 Released

Ruby 3.3.13 has been released.
Posted by **hsbt** on 23 Oct 2026

Ruby 3.4.12 Released

Ruby 3.4.12 has been released.
Posted by **nagachika** on 23 Oct 2026

Ruby 4.0.9 Released

Ruby 4.0.8 Released

Ruby 4.0.8 has been released.

Posted by **k0kubun** on 22 Oct 2026

[More News...](#) >



[Security](#) | [About This Website](#) | [About the Logo](#) | [News RSS](#) | [Ruby License](#)

[This website](#) is proudly maintained by members of the Ruby community.