KILLSWITCH · ISSUE #9 · 6 NOV 2026

The Patch Shipped. The Fix Didn't.

Check the runtime, not just the version number.

Killswitch rating: Check every self-built GitLab this week

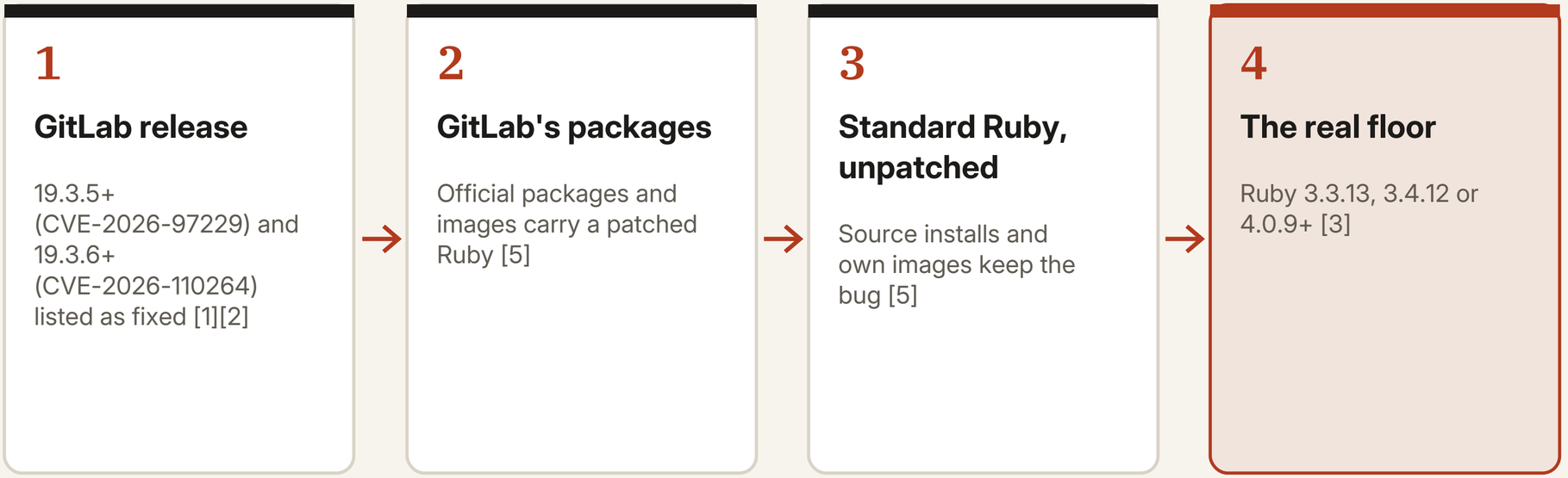
By Emmanuel Aigbehi Walstra

The Patch Shipped. The Fix Didn't.

Alpine upgraded GitLab to 19.3.6 and stayed exposed to CVE-2026-97229 [5].

- The fix is a Ruby patch, only in GitLab's own packages [5].
- Alpine's image ran standard Ruby [5].

Where the fix actually lives



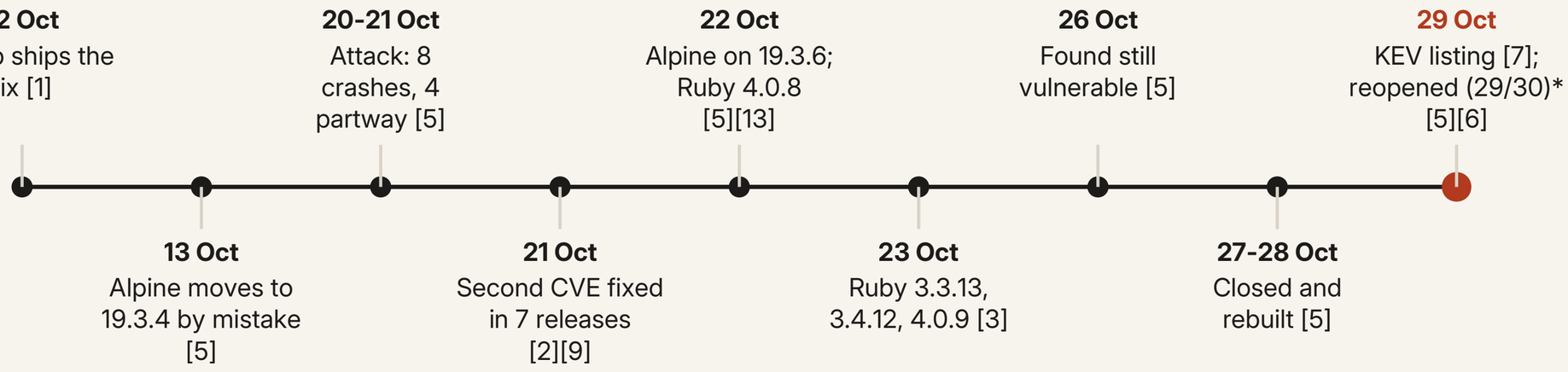
The bug is in Onigmo, Ruby's regex engine. GitLab patches Ruby in its own packages and images [5]. Standard Ruby got the fix on 22–23 Oct [3][13].

Two CVSS 10.0 regex flaws

- CVE-2026-97229: fixed 12 Oct; KEV since 29 Oct; its 1 Nov due date has passed [1][7][8].
- CVE-2026-110264: fixed 21 Oct, all versions from 7.0 [2][9].
- Both sit in Onigmo, Ruby's regex engine [3].

04 · OCTOBER

Patched on paper. Exposed for two weeks.



All dates Oct 2026. Alpine events from its incident post [5]. *Reopened (29/30): Alpine gives both dates; no time published [5][6].

Close, and not ruled out

- 8 worker crashes; 4 got partway [5].
- "We cannot rule it out, so we treated the instance as compromised" [5].
- Packages and releases checked: not tampered with [5].

The runtime is the patch

- Fixed in Ruby 4.0.8 (22 Oct); 3.4.12 · 3.3.13 · 4.0.9 (23 Oct) [3][13].
- "Regexp.timeout does not protect" [3].
- Ruby 3.2: end of life 1 Apr 2026, not in the fix list [3][17].

The bill for "cannot rule it out"

1 Reset for everyone

Passwords; 2FA, both authenticator apps and security keys; personal access tokens; feed and email tokens [6]

2 Re-entered by maintainers

CI/CD and pipeline schedule variable values, integration tokens; old values "may have been exposed" [6]

3 Replaced

New SSH host keys; webhook, push mirror and OAuth app secrets [6]

4 Kept

Your SSH keys and GPG keys; webhooks and mirrors were moved over [6]

What Alpine's users had to redo after the rebuild [6].

08 · ACT

Six checks for every GitLab

1. **Check the GitLab version**
   On a 21 Oct fixed release or later, for both CVEs [2]
2. **Check the Ruby under it**
   Own Ruby or own image: 3.3.13, 3.4.12 or 4.0.9+ [3][5]
3. **Re-pull your images**
   Check the Ruby inside the image, not just the tag [5]
4. **Run GitLab's detections**
   Look back to 12 Oct for worker crashes [1][2]
5. **Decide on compromise**
   If in doubt, rotate passwords, 2FA, tokens and secrets [5][6]
6. **Find other Ruby apps**
   Find other Ruby apps compiling user regexes [3][7]

Killswitch's own list. Defensive checks only.

Where this lives in your frameworks

Patch to the runtime	A.8.8, A.8.9, A.8.32 · NIS2 21(2)(e)
Know what you run	A.5.9 · NIS2 21(2)(i)
Secrets after a scare	A.5.15, A.5.17
Respond, and suppliers	A.5.26 · NIS2 21(2)(b), (d)

Killswitch's own mapping, not an official crosswalk. Check ISO titles against your licensed copy.

ISO/IEC 27001:2022 [11] · NIS2 [12]. Killswitch's own mapping, not an official crosswalk.

10 · STILL OPEN

What we don't know yet

- Why the first post named 19.3.4 [1][15][16].
- Whether the attack succeeded [5].
- The exact reopening date: 29 or 30 Oct [5][6].

Do this week

- GitLab on a 21 Oct fixed release or later [2].
- Ruby 4.0.9+ (4.0.8 fixed this CVE), 3.4.12 or 3.3.13 [3].
- Re-pull images; check the Ruby inside [5].
- Run GitLab's detections back to 12 Oct [1][2].
- Find other Ruby apps compiling user regexes [3][7].

Sources (1/2)

[1] GitLab: Critical Patch Release 19.4.2, 19.3.5, 19.2.8 (12 Oct 2026)
[2] GitLab: Critical Patch Release 19.5.1, 19.4.3, 19.3.6, 19.2.9, 19.1.9, 19.0.10, 18.11.13 (21 Oct 2026)
[3] Ruby: Regexp compilation fixes related to GitLab's CVE-2026-89078, CVE-2026-93577, CVE-2026-97229 and CVE-2026-110264 (23 Oct 2026)
[4] Ruby: Ruby 3.3.13 Released (23 Oct 2026)
[5] Alpine Linux: GitLab security incident: attempted exploitation of CVE-2026-97229 (28 Oct 2026, updated 30 Oct)
[6] Alpine Linux: GitLab is back: what you need to do (30 Oct 2026)
[7] CISA: Known Exploited Vulnerabilities Catalog, CVE-2026-97229 (added 29 Oct 2026)
[8] NVD: CVE-2026-97229
[9] NVD: CVE-2026-110264
[10] CERT-EU Security Advisory 2026-019: Critical Vulnerability in GitLab Community and Enterprise Editions (22 Oct 2026)
[11] ISO/IEC 27001:2022 Information security management systems
[12] NIS2 Directive (EU) 2022/2555, Article 21
[13] Ruby: Ruby 4.0.8 Released (22 Oct 2026)
[14] Ruby: Ruby 4.0.9 Released (23 Oct 2026)

Facts are from GitLab, Ruby, Alpine Linux, CISA, NVD and CERT-EU publications as read on 2 Nov 2026. No exploit detail is given. The checks and the framework mapping are Killswitch's own, not an official crosswalk.

Sources (2/2)

[15] Wayback Machine: GitLab 12 Oct patch post, earlier capture on 12 Oct 2026 (names 19.3.4)

[16] Wayback Machine: the same post, later capture on 12 Oct 2026 (names 19.3.5)

[17] Ruby: Ruby Maintenance Branches (Ruby 3.2 end of life 1 Apr 2026)

Facts are from GitLab, Ruby, Alpine Linux, CISA, NVD and CERT-EU publications as read on 2 Nov 2026. No exploit detail is given. The checks and the framework mapping are Killswitch's own, not an official crosswalk.

FROM THE PUBLISHERS OF KILLSWITCH

Track your patches down to the runtime, with the evidence

GRCOMPLIANCE

Keep your asset inventory, patch records and incident controls, owners and evidence in one place, mapped to ISO 27001 and NIS2.

Try the live demo →

demo.grcompliance.com

Self-host free: github.com/Sectutor/GRCompliance-Core

SECTUTOR

Security and GRC books, training and audit kits.

sectutor.com

Emmanuel Aigbehi Walstra is a CISO who also serves as a virtual CISO (vCISO) for several organisations, with 30+ years in cybersecurity, 10,000+ people trained, and author of the CCSP Excellence books.