Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Ruby2Shell: Ruby Heap Overflow Carries Conditional RCE Risk

Date of Publication	Admiralty Code	TA Number
November 20, 2026	A1	TA2026347

Summary

First Seen: November 18, 2026
Affected Products: Ruby, GitLab, GitHub Enterprise Server, Chatwoot, AWS Elastic Beanstalk, Amazon Linux 2023
Impact: Ruby2Shell (CVE-2026-132825) lets attackers corrupt heap memory in Ruby applications simply by getting crafted, legacy-encoded text passed through a routine case-conversion call. Rails and classic-style Sinatra applications are exposed by default without authentication, and GitLab, GitHub Enterprise Server, Chatwoot, and AWS Elastic Beanstalk ship affected runtimes. A successful attack runs code with the application server's privileges, exposing source code, credentials, CI/CD secrets, and customer data, and even failed attempts crash the Ruby process. Because reliable exploitation needs precise heap control, the practical risk for most applications is moderate, so internet-facing services handling untrusted input and end-of-life Ruby versions that will never be patched should be fixed first.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-132825	(Ruby2Shell) Ruby Heap Buffer Overflow in String Case Conversion Vulnerability	Ruby	✗	✗	✓

Vulnerability Details

#1

CVE-2026-132825, dubbed Ruby2Shell, is a heap-based buffer overflow (CWE-122) in Ruby's string case-conversion routine for legacy single-byte encodings such as ISO-8859-1 and Windows-1252. Disclosed on November 18, 2026, as one of seven memory-safety flaws in Ruby's regular expression engine and string handling, it is rated Critical by the Ruby project, which confirms proofs of concept achieving remote code execution in some scenarios.

#2

An off-by-one error (CWE-193) mishandles the German sharp-s (ß): upcasing it produces two bytes ("SS"), but the loop checks for only one byte of space. A string with 21 ß characters overflows the buffer's 20-byte slack by one byte, writing "S" (0x53) or "s" (0x73) past its end and triggering an out-of-bounds read when the result is copied. UTF-8 strings use a separate, unaffected code path. The fix checks for more than one byte of room before writing the expansion.

#3

The flaw is reached through upcase, swapcase, capitalize, downcase(:fold), and casecmp?, which applications use to normalize headers, parameters, and identifiers. An attacker controls the input length, and therefore the size of the targeted heap allocation, enabling the heap grooming needed to turn the one-byte overwrite into code execution. Rails and classic-style Sinatra apps are reachable by default without authentication; other frameworks and plain Rack are exposed only through custom code.

#4

GitLab, GitHub Enterprise Server, and Chatwoot bundle vulnerable runtimes, while Mastodon, OpenProject, and Discourse already ship a fix. AWS confirms its Elastic Beanstalk Ruby platforms and the Amazon Linux 2023 ruby3.2, ruby3.4, and ruby4.0 packages are affected (the Amazon Linux 2 Ruby 2.0 package is not) and has begun releasing updates. End-of-life Ruby branches will not be fixed. The MITRE CNA scores the flaw CVSS 7.4 (High), and there is no exploitation in the wild. Proofs of concept exist and a public exploit release is planned, but no weaponized exploit against real-world applications has been shown, and exploitation needs target-specific heap grooming, with each failed attempt crashing the process. Measured patching, starting with internet-facing applications, is warranted.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-132825	Ruby (before 3.3.14, 3.4.0–3.4.12, 4.0.0–4.0.9; EOL ≤3.2 unfixed) GitLab (19.6.0 and earlier releases bundling affected Ruby) GitHub Enterprise Server (3.22.5 and earlier bundling affected Ruby) Chatwoot (4.20.0 and earlier) AWS Elastic Beanstalk Amazon Linux 2023 Ruby platforms before 4.15.4 Amazon Linux 2023 ruby3.2, ruby3.4, ruby4.0 packages	cpe:2.3:a:ruby-lang:ruby:*:*:*:*:*:*:*:*:*, cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:*:*, cpe:2.3:a:github:enterprise_server:*:*:*:*:*:*:*:*:*, cpe:2.3:a:chatwoot:chatwoot:*:*:*:*:*:*:*:*:*, cpe:2.3:a:amazon:elastic_beanstalk:*:*:*:*:*:*:*:*:*, cpe:2.3:o:amazon:amazon_linux:*:*:*:*:*:*:*:*:*	CWE-122, CWE-193

Recommendations

Maintain a Runtime Inventory: Keep an up-to-date inventory of all Ruby runtimes in use, including background workers, container base images, distribution packages, and vendor products that ship their own Ruby, such as GitLab and GitHub Enterprise Server. Track upstream Ruby security announcements so that critical runtime flaws can be identified and prioritized as soon as they are disclosed.

Retire End-of-Life Ruby Versions: Ruby 3.2 and earlier will not receive a fix for this flaw. Migrate these workloads to a supported release and, until migration is complete, isolate them from untrusted networks and restrict access to them.

Normalize Untrusted Input Encodings: Review application code that calls upcase, swapcase, downcase(:fold), or casecmp? on user-controlled data, and convert untrusted input to UTF-8 before case conversion. UTF-8 uses an unaffected code path, which removes the exposure even if a vulnerable runtime is temporarily left in place.

Upgrade Ruby and Verify: Upgrade all Ruby runtimes to a fixed release, prioritizing internet-facing Rails and classic-style Sinatra applications that pass untrusted input to case-conversion or regular expression routines. Rebuild container images, restart application processes, and confirm the Ruby version reported by the running process rather than only the installed package.

Patch Bundled and Managed Platforms: Install vendor-fixed releases of self-hosted software that ships its own Ruby, such as GitLab, GitHub Enterprise Server, and Chatwoot. On AWS, move Elastic Beanstalk environments to the updated Amazon Linux 2023 Ruby platform (version 4.15.4) and apply the updated ruby3.2, ruby3.4, and ruby4.0 packages on Amazon Linux 2023 once they are published in the Amazon Linux Security Center. Upgrading the system Ruby does not fix applications that bundle their own interpreter, so verify the embedded Ruby version after each update.

Apply Least Privilege and Segmentation: Run Ruby application servers under dedicated low-privilege accounts, restrict their outbound network access, and segment them from sensitive internal systems. This limits the blast radius if an attacker converts the overflow into code execution.

Deploy Interim Request Filtering: Until patching is complete, configure WAF or reverse-proxy rules to flag or block requests that declare legacy single-byte charsets and contain long runs of the sharp-s character. AWS WAF users should enable version 1.29 or later of the AWS Managed Rules Known Bad Inputs rule group, which includes rules targeting exploitation attempts for this vulnerability. No workaround fully mitigates the flaw, so limit internet exposure of unpatched Ruby applications and treat filtering as a temporary safeguard, not a substitute for upgrading.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Impact	T1499: Endpoint Denial of Service	T1499.004: Application or System Exploitation

Patch Link

https://github.com/ruby-git/ruby-git/releases

References

https://www.ruby-lang.org/en/news/2026/11/18/multiple-vulnerabilities-in-regexp-and-string/

https://github.com/ruby/ruby/security/advisories/GHSA-34m4-m9fh-gqp5

https://verialabs.com/ruby2shell/

https://www.ox.security/blog/ruby2shell-ruby-memory-corruption-flaws-expose-applications-to-remote-code-execution-but-is-it-an-actual-risk/

https://aws.amazon.com/security/security-bulletins/2026-193-aws/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

November 20, 2026 • 07:00 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com