



bcrypt-ruby has an Integer Overflow that Causes Zero Key-Strengthening Iterations at Cost=31 on JRuby

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2026-33306 |
| State | PUBLISHED |
| Assigner | GitHub_M |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-03-24 01:17:02 UTC |
| Updated | 2026-03-30 14:07:23 UTC |

Description bcrypt-ruby is a Ruby binding for the OpenBSD bcrypt() password hashing algorithm. Prior to version 3.1.22, an integer ove

Risk And Classification

Primary CVSS: v4.0 4.5 MEDIUM from security-advisories@github.com

CVSS:4.0/AV:L/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000200000 probability, percentile 0.051340000 (date 2026-04-01)

Problem Types: CWE-190 | CWE-190 CWE-190: Integer Overflow or Wraparound

| Version | Source | Type | Score | Severity | Vector |
|---------|--------------------------------|-----------|-------|----------|--|
| 4.0 | security-advisories@github.com | Secondary | 4.5 | MEDIUM | CVSS:4.0/AV:L/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X |
| 4.0 | CNA | DECLARED | 4.5 | MEDIUM | CVSS:4.0/AV:L/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X |
| 3.1 | nvd@nist.gov | Primary | 7.5 | HIGH | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N |

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

High

Attack Requirements

Present

Privileges Required

None

User Interaction

None

Confidentiality

High

Integrity

High

Availability

None

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|---------------------|-------------|---------|--------|---------|----------|
| Application | Bcrypt-ruby Project | Bcrypt-ruby | All | All | All | All |

Vendor Declared Affected Products

| Source | Vendor | Product | Version | Platforms |
|--------|---------------------|-------------|---------------|----------------|
| CVE | Bcrypt-ruby Project | Bcrypt-ruby | 2.0.0 - 2.1.0 | Linux, Windows |

References

| Reference | Source | Link | Tags |
|---|--------------------------------|---|----------|
| github.com/bcrypt-ruby/bcrypt-ruby/security/advisories/GHSA-f27w-vcwj-c954 | security-advisories@github.com | github.com | Mitigati |
| github.com/bcrypt-ruby/bcrypt-ruby/commit/831ce64cb0a9502130fa93a28bfd95... | security-advisories@github.com | github.com | Patch |
| github.com/bcrypt-ruby/bcrypt-ruby/releases/tag/v3.1.22 | security-advisories@github.com | github.com | Produc |
| CVE Program record | CVE.ORG | www.cve.org | canonic |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonic |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](https://mitre.org/licenses).

CVE.report and Source URL Uptime Status status.cve.report