ERB has an @_init deserialization guard bypass via def_module / def_method / def_class

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-41316
State	PUBLISHED
Assigner	GitHub_M
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-24 03:16:11 UTC
Updated	2026-04-24 14:50:56 UTC
Description	ERB is a templating system for Ruby. Ruby 2.7.0 (before ERB 2.2.0 was published on rubygems.org) introduced an `@_init

Risk And Classification

Primary CVSS: v3.1 8.1 HIGH from security-advisories@github.com

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

Problem Types: CWE-693 | CWE-693 CWE-693: Protection Mechanism Failure

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	DECLARED	8.1	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Ruby	Erb	affected < 4.0.3.1	Not specified
CNA	Ruby	Erb	affected = 4.0.4	Not specified
CNA	Ruby	Erb	affected >= 5.0.0, < 6.0.1.1	Not specified
CNA	Ruby	Erb	affected >= 6.0.2, < 6.0.4	Not specified

References

Reference	Source	Link	Tags
github.com/ruby/erb/security/advisories/GHSA-q339-8rmv-2mhv	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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