



# Rails Active Storage has a possible DoS vulnerability in proxy mode via multi-range requests

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

## Summary

<b>CVE</b>	CVE-2026-33658
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-26 22:16:29 UTC
<b>Updated</b>	2026-03-30 13:26:50 UTC
<b>Description</b>	Active Storage allows users to attach cloud and local files in Rails applications. Prior to versions 8.1.2.1, 8.0.4.1, and 7.2.3.

## Risk And Classification

**Primary CVSS:** v4.0 2.3 LOW from security-advisories@github.com

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:N/VA:H/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:** 0.000500000 probability, percentile 0.156250000 (date 2026-04-01)

**Problem Types:** CWE-770 | CWE-770 CWE-770: Allocation of Resources Without Limits or Throttling

Version	Source	Type	Score	Severity	Vector
4.0	security-advisories@github.com	Secondary	2.3	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/S
4.0	CNA	DECLARED	2.3	LOW	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/S

## CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

Present

Privileges Required

Low

User Interaction

None

None
Confidentiality
None
Integrity
None
Availability
High
Sub Conf.
None
Sub Integrity
None
Sub Availability
None

CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:N/VA:H/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

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Rails	Activestorage	affected >= 8.1.0, < 8.1.2.1	Not specified
CNA	Rails	Activestorage	affected >= 8.0.0, < 8.0.4.1	Not specified
CNA	Rails	Activestorage	affected < 7.2.3.1	Not specified

#### References

Reference	Source	Link	Tags
github.com/rubysec/ruby-advisory-db/blob/master/gems/activestorage/CVE-2...	security-advisories@github.com	github.com	
github.com/rails/rails/security/advisories/GHSA-p9fm-f462-ggrg	security-advisories@github.com	github.com	
github.com/rails/rails/releases/tag/v7.2.3.1	security-advisories@github.com	github.com	
github.com/rails/rails/releases/tag/v8.0.4.1	security-advisories@github.com	github.com	
github.com/rails/rails/releases/tag/v8.1.2.1	security-advisories@github.com	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)**