



CVE-2020-5249

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2020-5249
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-03-02 16:15:00 UTC
Updated	2023-11-07 03:23:00 UTC
Description	In Puma (RubyGem) before 4.3.3 and 3.12.4, if an application using Puma allows untrusted input in an early-hints header, a

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Puma	Puma	All	All	All	All
Application	Puma	Puma	All	All	All	All

References

Reference	Source	Link
HTTP Response Splitting · Advisory · puma/puma · GitHub	MISC	github.com
[SECURITY] Fedora 31 Update: rubygem-puma-3.12.4-1.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.or
[SECURITY] Fedora 30 Update: rubygem-puma-3.12.4-1.fc30 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.or
[SECURITY] Fedora 32 Update: rubygem-puma-4.3.3-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.or
[SECURITY] Fedora 30 Update: rubygem-puma-3.12.4-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.or
HTTP Injection - fix bug + 1 more vector (#2136) · puma/puma@c22712f · GitHub	MISC	github.com
HTTP Response Splitting (Early Hints) · Advisory · puma/puma · GitHub	CONFIRM	github.com
HTTP Response Splitting Software Attack OWASP Foundation	MISC	owasp.org
[SECURITY] Fedora 32 Update: rubygem-puma-4.3.3-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.or
[SECURITY] Fedora 31 Update: rubygem-puma-3.12.4-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.or
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[750577](#) OpenSUSE Security Update for rmt-server (openSUSE-SU-2020:2000-1)

[750580](#) OpenSUSE Security Update for rmt-server (openSUSE-SU-2020:1993-1)

© [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](#) 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](#)