



# CVE-2021-41136

Published on: 10/12/2021 12:00:00 AM UTC

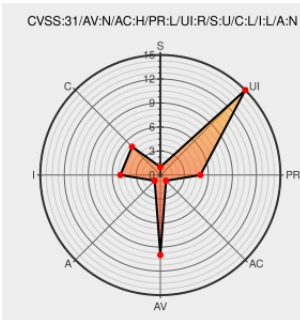
Last Modified on: 10/27/2021 03:21:00 PM UTC

## CVE-2021-41136 - advisory for GHSA-48w2-rm65-62xx

Source: Mitre

Source: Nist

Print: PDF



Certain versions of **Puma** from **Puma** contain the following vulnerability:

Puma is a HTTP 1.1 server for Ruby/Rack applications. Prior to versions 5.5.1 and 4.3.9, using `puma` with a proxy which forwards HTTP header values which contain the LF character could allow HTTP request smuggling. A client could smuggle a request through a proxy, causing the proxy to send a response back to another unknown client.

The only proxy which has this behavior, as far as the Puma team is aware of, is Apache Traffic Server. If the proxy uses persistent connections and the client adds another request in via HTTP pipelining, the proxy may mistake it as the first request's body. Puma, however, would see it as two requests, and when processing the second request, send back a response that the proxy does not expect. If the proxy has reused the persistent connection to Puma to send another request for a different client, the second response from the first client will be sent to the second client. This vulnerability was patched in Puma 5.5.1 and 4.3.9. As a workaround, do not use Apache Traffic Server with `puma`.

CVE-2021-41136 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **LOW** severity.

Affected Vendor/Software: **puma** - **puma** version  $\geq 5.0.0$ ,  $< 5.5.1$

Affected Vendor/Software: **puma** - **puma** version  $< 4.3.9$

CVSS3 Score: **3.7 - LOW**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>NETWORK</b>	<b>HIGH</b>	<b>LOW</b>	<b>REQUIRED</b>
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
<b>UNCHANGED</b>	<b>LOW</b>	<b>LOW</b>	<b>NONE</b>

CVSS2 Score: **3.6 - LOW**

Access Access Authentication

<b>Vector</b>	<b>Complexity</b>	
<b>NETWORK</b>	<b>HIGH</b>	<b>SINGLE</b>
<b>Confidentiality Impact</b>	<b>Integrity Impact</b>	<b>Availability Impact</b>
<b>PARTIAL</b>	<b>PARTIAL</b>	<b>NONE</b>

## CVE References

Description	Tags	Link
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') in puma · Advisory · puma/puma · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	CONFIRM <a href="https://github.com/puma/puma/security/advisories/GHSA-48w2-rm65-62xx">github.com/puma/puma/security/advisories/GHSA-48w2-rm65-62xx</a>
Merge pull request from GHSA-48w2-rm65-62xx · puma/puma@acdc3ae · GitHub	<a href="#">github.com</a> <a href="#">text/html</a>	MISC <a href="https://github.com/puma/puma/commit/acdc3ae571dfae0e045cf09a295280127db65c7f">github.com/puma/puma/commit/acdc3ae571dfae0e045cf09a295280127db65c7f</a>

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Puma	Puma	All	All	All	All
Application	Puma	Puma	All	All	All	All
<code>cpe:2.3:a:puma:puma:*:*:*:*:ruby:*:*</code>						
<code>cpe:2.3:a:puma:puma:*:*:*:*:ruby:*:*</code>						

No vendor comments have been submitted for this CVE

## Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-41136 : Puma is a HTTP 1.1 server for Ruby/Rack applications. Prior to versions 5.5.1 and 4.3.9, using `pu... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a>	2021-10-12 15:34:48
@rubylandnews	RubySec → CVE-2021-41136 (puma): Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') in puma <a href="https://rubysec.com/advisories/CVE...">rubysec.com/advisories/CVE...</a>	2021-10-12 18:25:04

[← Previous ID](#)

[Next ID →](#)

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](#)**