



CVE-2017-11173

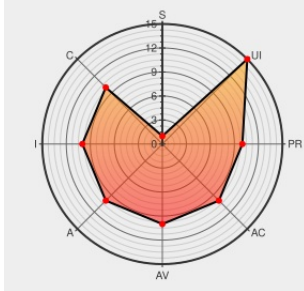
Published on: 07/12/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:25 PM UTC

CVE-2017-11173

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H



Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

Missing anchor in generated regex for rack-cors before 0.4.1 allows a malicious third-party site to perform CORS requests. If the configuration were intended to allow only the trusted example.com domain name and not the malicious example.net domain name, then example.com.example.net (as well as example.com-example.net)

would be inadvertently allowed.

CVE-2017-11173 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Full Disclosure: CVE-2017-11173 Missing anchor in generated regex for rack-cors before 0.4.1	Mailing List Third Party Advisory	MISC seclists.org/fulldisclosure/2017/Jul/22

allows a malicious third-party site to perform CORS requests	seclists.org text/html	
Add end string anchor to string origin def · cyu/rack-cors@42ebe6c · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/cyu/rack-cors/commit/42ebe6caa8e85ffa9c8a171bda668ba1acc7a5e6
Debian -- Security Information -- DSA-3931-1 ruby-rack-cors	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-3931
rack-cors Missing Anchor ≈ Packet Storm	Third Party Advisory VDB Entry packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/143345/rack-cors-Missing-Anchor.html

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Rack-cors Project	Rack-cors	All	All	All	All
Application	Rack-cors Project	Rack-cors	All	All	All	All
cpe:2.3:o:debian:debian_linux:9.0:****:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:****:*:*:						
cpe:2.3:a:rack-cors_project:rack-cors:****:*:ruby:*:*:						
cpe:2.3:a:rack-cors_project:rack-cors:****:*:ruby:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)