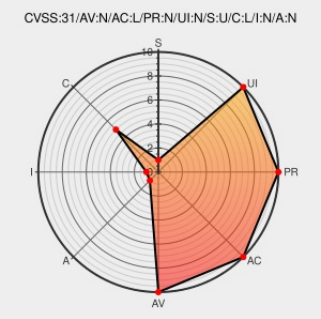
# CVE-2019-18978

Published on: 11/14/2019 12:00:00 AM UTC

Last Modified on: 05/21/2021 04:47:00 PM UTC

## CVE-2019-18978

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

An issue was discovered in the rack-cors (aka Rack CORS Middleware) gem before 1.0.4 for Ruby. It allows ../ directory traversal to access private resources because resource matching does not ensure that pathnames are in a canonical format.

CVE-2019-18978 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

### CVSS3 Score: 5.3 - MEDIUM

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | NONE | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | LOW | NONE | NONE |

### CVSS2 Score: 5 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | NONE | NONE |

### CVE References

| Description | Tags | Link |
|---|---|---|
| USN-4571-1: rack-cors vulnerability \| Ubuntu security notices \| Ubuntu | usn.ubuntu.com, text/html | UBUNTU USN-4571-1 |
| Unescape and resolve paths before resource checks · cyu/rack-cors@e4d4fc3 · GitHub | Patch, github.com | MISC github.com/cyu/rack-cors/commit/e4d4fc362a4315808927011cbe5afcfe5486f17d |

| | | |
|---|---|---|
| | text/html | |
| [SECURITY] [DLA 2096-1] ruby-rack-cors security update | lists.debian.org<br>text/html | MLIST [debian-lts-announce] 20200206 [SECURITY] [DLA 2096-1] ruby-rack-cors security update |
| Comparing v1.0.3...v1.0.4 · cyu/rack-cors · GitHub | Patch<br>github.com<br>text/html | MISC github.com/cyu/rack-cors/compare/v1.0.3...v1.0.4 |
| [SECURITY] [DLA 2389-1] ruby-rack-cors security update | lists.debian.org<br>text/html | MLIST [debian-lts-announce] 20201001 [SECURITY] [DLA 2389-1] ruby-rack-cors security update |
| Debian -- Security Information -- DSA-4918-1 ruby-rack-cors | www.debian.org<br>Depreciated Link<br>text/html | DEBIAN DSA-4918 |

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.

## Related QID Numbers

178604 Debian Security Update for ruby-rack-cors (DSA 4918-1)

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Debian | Debian Linux | 10.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | 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:canonical:ubuntu_linux:16.04:*:*:*:esm:*:*:*:

cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

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

## Social Mentions

Social Mentions

| Source | Title | Posted (UTC) |
| --- | --- | --- |
| @LinInfoSec | Ruby - CVE-2019-18978: github.com/cyu/rack-cors/… | 2021-05-19 05:20:45 |

← Previous ID

Next ID→

© CVE.report 2023 |
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 registred 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**