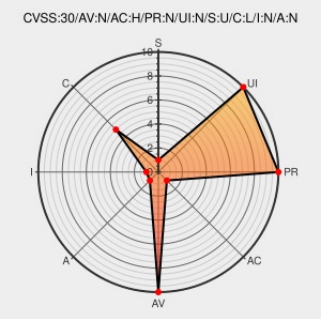
CVE-2018-3759

Published on: 06/13/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:25 PM UTC

CVE-2018-3759

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



Certain versions of Private Address Check from Private Address Check Project contain the following vulnerability:

private_address_check ruby gem before 0.5.0 is vulnerable to a time-of-check time-of-use (TOCTOU) race condition due to the address the socket uses not being checked. DNS entries with a TTL of 0 can trigger this case where the initial resolution is a public address but the subsequent resolution is a private address.

CVE-2018-3759 has been assigned by support@hackerone.com to track the vulnerability - currently rated as LOW severity.

Affected Vendor/Software: **HackerOne** - **private_address_check ruby gem** version **0.5.0**

CVSS3 Score: 3.7 - LOW

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Fix TOCTOU bug ·	Patch	MISC

jtdowney/private_address_check@4068228 · GitHub	Third Party Advisory github.com text/html	github.com/jtdowney/private_address_check/commit/4068228187db87fea

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
Application	Private Address Check Project	Private Address Check	All	All	All	All
Application	Private Address Check Project	Private Address Check	All	All	All	All

cpe:2.3:a:private_address_check_project:private_address_check:*:*:*:*:*:ruby:*:*:

cpe:2.3:a:private_address_check_project:private_address_check:*:*:*:*:*:ruby:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→