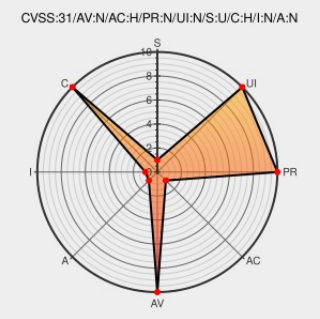
CVE-2020-15235

Published on: 10/05/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:41 PM UTC

CVE-2020-15235 - advisory for GHSA-ph67-c355-52vm

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



Certain versions of Core from Ractf contain the following vulnerability:

In RACTF before commit f3dc89b, unauthenticated users are able to get the value of sensitive config keys that would normally be hidden to everyone except admins. All versions after commit f3dc89b9f6ab1544a289b3efc06699b13d63e0bd(3/10/20) are patched.

CVE-2020-15235 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **ractf** - **core** version **< f3dc89b**

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	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
patch unauthenticated users being able to read sensitive config field… · ractf/core@f3dc89b · GitHub	Patch Vendor Advisory github.com	MISC github.com/ractf/core/commit/f3dc89b9f6ab1544a289b3efc06699b13d63e0bd

	text/html	
Unauthenticated Users Can View Sensitive Config Keys · Advisory · ractf/core · GitHub	Vendor Advisory github.com text/html	CONFIRM github.com/ractf/core/security/advisories/GHSA-ph67-c355-52vm

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	Ractf	Core	All	All	All	All

cpe:2.3:a:ractf:core:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→