



CVE-2021-32773

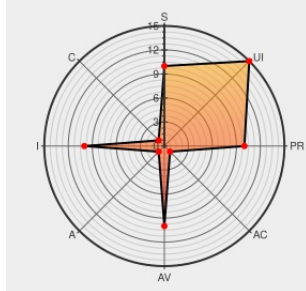
Published on: 07/19/2021 12:00:00 AM UTC

Last Modified on: 07/29/2021 04:22:00 PM UTC

CVE-2021-32773 - advisory for GHSA-cgrw-p7p7-937c

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

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



Certain versions of [Racket](#) from [Racket-lang](#) contain the following vulnerability:

Racket is a general-purpose programming language and an ecosystem for language-oriented programming. In versions prior to 8.2, code evaluated using the Racket sandbox could cause system modules to incorrectly use attacker-created modules instead of their intended dependencies. This could allow system functions to be controlled by

the attacker, giving access to facilities intended to be restricted. This problem is fixed in Racket version 8.2. A workaround is available, depending on system settings. For systems that provide arbitrary Racket evaluation, external sandboxing such as containers limit the impact of the problem. For multi-user evaluation systems, such as the `handin-server` system, it is not possible to work around this problem and upgrading is required.

CVE-2021-32773 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [racket](#) - **racket** version < 8.2

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	NONE	HIGH	NONE

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact

NONE

PARTIAL

NONE

CVE References

Description	Tags	Link
racket/sandbox: documentation and tests for reader and require checking · racket/racket@6ca4ffe · GitHub	github.com text/html	 MISC github.com/racket/racket/commit/6ca4ffeca1e5877d44f835760ad89f18488d97e1
Confused deputy attack in sandbox module resolution · Advisory · racket/racket · GitHub	github.com text/html	 CONFIRM github.com/racket/racket/security/advisories/GHSA-cgrw-p7p7-937c

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

179462 Debian Security Update for racket (CVE-2021-32773)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Racket-lang	Racket	All	All	All	All
cpe:2.3:a:racket-lang:racket:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-32773 : Racket is a general-purpose programming language and an ecosystem for language-oriented programmin... twitter.com/i/web/status/1...	2021-07-20 00:01:00
 @SecRiskRptSME	RT: CVE-2021-32773 Racket is a general-purpose programming language and an ecosystem for language-oriented program... twitter.com/i/web/status/1...	2021-07-20 07:21:32
 /r/netcve	CVE-2021-32773	2021-07-20 00:40:23

[← 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 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](#).

