



# CVE-2021-41641

Published on: Not Yet Published

Last Modified on: 06/21/2022 02:47:00 PM UTC

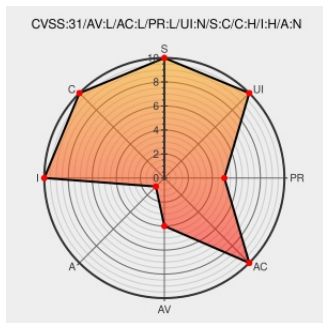
## CVE-2021-41641

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Deno <=1.14.0 file sandbox does not handle symbolic links correctly. When running Deno with specific write access, the Deno.symlink method can be used to gain access to any directory.

CVE-2021-41641 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.4 - HIGH**

| Attack Vector | Attack Complexity      | Privileges Required | User Interaction    |
|---------------|------------------------|---------------------|---------------------|
| LOCAL         | LOW                    | LOW                 | NONE                |
| Scope         | Confidentiality Impact | Integrity Impact    | Availability Impact |
| CHANGED       | HIGH                   | HIGH                | NONE                |

CVSS2 Score: **3.6 - LOW**

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

## CVE References

| Description                                                            | Tags                                                        | Link                                                                                   |
|------------------------------------------------------------------------|-------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Hackers Report                                                         | <a href="#">hackers.report</a><br><a href="#">text/html</a> | <a href="#">MISC</a><br><a href="#">hackers.report/report/614876917a7b150012836bb8</a> |
| [Security] Deno Sandbox Escape · Issue #12152 · denoland/deno · GitHub | <a href="#">github.com</a><br><a href="#">text/html</a>     | <a href="#">MISC</a> <a href="#">github.com/denoland/deno/issues/12152</a>             |

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](mailto: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                    | <a href="#">Deno</a> | <a href="#">Deno</a> | All     | All    | All     | All      |
| cpe:2.3:a:deno:deno:*:*:*:*:*: |                      |                      |         |        |         |          |

No vendor comments have been submitted for this CVE

#### Social Mentions

| Source                                                                                       | Title                                                                                                                                                                                                          | Posted (UTC)        |
|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|  @CVEreport  | CVE-2021-41641 : Deno <=1.14.0 file sandbox does not handle symbolic links correctly. When running Deno with specif... <a href="https://twitter.com/i/web/status/1408123456">twitter.com/i/web/status/1...</a> | 2022-06-12 13:05:18 |
|  /r/netcve | <a href="#">CVE-2021-41641</a>                                                                                                                                                                                 | 2022-06-12 13:38:19 |

[← 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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)