



CVE-2023-3891

Published on: Not Yet Published

Last Modified on: 09/20/2023 06:55:00 PM UTC

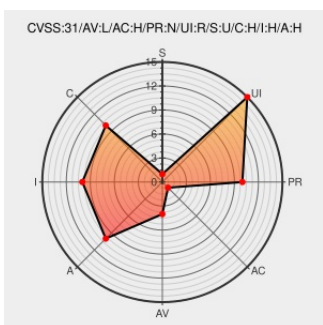
CVE-2023-3891

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Race condition in Lapce v0.2.8 allows an attacker to elevate privileges on the system

CVE-2023-3891 has been assigned by [fluidattacks.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [fluidattacks.com](#) **Lapce** - **Lapce** version = **0.2.8**

CVSS3 Score: **7 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	HIGH	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Lapce	lapce.dev text/html	MISC lapce.dev
Lapce v0.2.8 - Privilege escalation via Race Condition Fluid Attacks	fluidattacks.com text/html	MISC fluidattacks.com/advisories/aerosmith

By selecting these links, you may be leaving CVEreport workspace. 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	Lapce	Lapce	0.2.8	All	All	All
cpe:2.3:a:lapce:lapce:0.2.8:*:*:*:*:*::						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID→		