

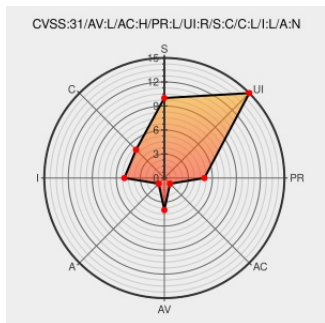


CVE-2021-32830

Published on: 08/17/2021 12:00:00 AM UTC

Last Modified on: 08/25/2021 02:00:00 AM UTC

CVE-2021-32830 - advisory for GHSL-2021-061

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

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

The `@diez/generation` npm package is a client for Diez. The `locateFont` method of `@diez/generation` has a command injection vulnerability. Clients of the `@diez/generation` library are unlikely to be aware of this, so they might unwittingly write code that contains a vulnerability. This issue may lead to remote code execution if a client of the library calls the vulnerable method with untrusted input. All versions of this package are vulnerable as of the writing of this CVE.

CVE-2021-32830 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [diez](#) - **diez** version **all**

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

CVSS2 Score: **6.8 - MEDIUM**

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

CVE References

Description	Tags	Link
GitHub - diez/diez: The Design Token Framework — Adopt a unified design language across platforms, codebases, and teams	github.com text/html	MISC github.com/diez/diez
@diez/generation - npm	www.npmjs.com text/html	MISC www.npmjs.com/package/@diez/generation
GHSL-2021-061: Command injection in @diez/generation - CVE-2021-32830 GitHub Security Lab	securitylab.github.com text/html	CONFIRM securitylab.github.com/advisories/GHSL-2021-061-diez-generation-cmd-injection/

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

[981264](#) Nodejs (npm) Security Update for @diez/generation (GHSA-8c3f-x5f9-6h62)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Haikuforteams	Diez	-	All	All	All
cpe:2.3:a:haikuforteams:diez:-:*:*:*:*:node.js:*:*						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@GHSecurityLab	GHSL-2021-061: Command injection in diez/generation - CVE-2021-32830 github.co/3zov2XE	2021-07-21 19:00:17
@CVEreport	CVE-2021-32830 : The @diez/generation npm package is a client for Diez. The locateFont method of @diez/generation h... twitter.com/i/web/status/1...	2021-08-17 18:01:47

[← 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](#)