


Improper Handling of Unexpected Data Type in ced

High sonicdoe published GHSA-27wq-qx3q-fxm9 on Aug 17, 2021

Package

 **ced** (npm)

Affected versions

0.1.0

Patched versions

1.0.0

Description

Impact

In ced v0.1.0, passing data types other than `Buffer` causes the Node.js process to crash.

Patches

The problem has been patched in [ced v1.0.0](#). You can upgrade from v0.1.0 without any breaking changes.

Workarounds

Before passing an argument to ced, verify it's a `Buffer` using `Buffer.isBuffer(obj)`.

CVSS score

[CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/RL:O/RC:C](#)

Base Score: 7.5 (High)
Temporal Score: 7.2 (High)

Since ced is a library, the scoring is based on the "reasonable worst-case implementation scenario", namely, accepting data from untrusted sources over a network and passing it directly to ced. Depending on your specific implementation, the vulnerability's severity in your program may be different.

Proof of concept

```
const express = require("express");
const bodyParser = require("body-parser");
const ced = require("ced");

const app = express();

app.use(bodyParser.raw());

app.post("/", (req, res) => {
  const encoding = ced(req.body);

  res.end(encoding);
});

app.listen(3000);
```

`curl --request POST --header "Content-Type: text/plain" --data foo http://localhost:3000` crashes the server.

References

- [a4d9f10](#)

Severity

High 7.5 / 10

CVSS base metrics	
Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	None
Availability	High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE ID

CVE-2021-39131

Weaknesses

CWE-241

Credits



cristianstaicu