

Missing Release of Memory after Effective Lifetime in detect-character-encoding

High sonicdoe published GHSA-5rwj-j5m3-3chj on Aug 31, 2021

Package

 detect-character-encoding (npm)

Affected versions

0.3.0

Patched versions

0.3.1

Description

Impact

In detect-character-encoding v0.3.0 and earlier, allocated memory is not released.

Patches

The problem has been patched in [detect-character-encoding v0.3.1](#).

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, using detect-character-encoding in a program accessible over the internet which becomes unavailable when running out of memory. Depending on your specific implementation, the vulnerability's severity in your program may be different.

Proof of concept

```
const express = require("express");
const detectCharacterEncoding = require("detect-character-encoding");

const app = express();

app.get("/", (req, res) => {
  detectCharacterEncoding(Buffer.from("foo"));

  res.end();
});

app.listen(3000);
```

hey -n 1000000 http://localhost:3000 ([hey](#)) causes the Node.js process to consume more and more memory.

References

- [d443569](#)
- [#6](#)

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-2021-39176

Weaknesses

CWE-401