CVE-2021-39176

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-39176
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-08-31 18:15:00 UTC
Updated	2021-09-08 17:30:00 UTC
Description	detect-character-encoding is a package for detecting character encoding using ICU. In detect-character-encoding v0.3.0 an

Risk And Classification

Problem Types: CWE-401

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Detect-character-encoding Project	Detect-character-encoding	All	All	All	All

References

Reference	S
Fix memory leak by properly closing `charsetDetector` · sonicdoe/detect-character-encoding@d443569 · GitHub	M
Fix memory leak by properly closing charsetDetector by mhertsch · Pull Request #6 · sonicdoe/detect-character-encoding · GitHub	M
Missing Release of Memory after Effective Lifetime in detect-character-encoding · Advisory · sonicdoe/detect-character-encoding · GitHub	C
Release v0.3.1 · sonicdoe/detect-character-encoding · GitHub	M
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980378 Nodejs (npm) Security Update for detect-character-encoding (GHSA-5rwj-j5m3-3chj)

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report