



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	
Fix memory leak by properly closing `charsetDetector` · sonicdoe/detect-character-encoding@d443569 · GitHub	S
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	M

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)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)