



CVE-2020-4077

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-4077
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-07-07 00:15:00 UTC
Updated	2020-07-13 19:51:00 UTC
Description	In Electron before versions 7.2.4, 8.2.4, and 9.0.0-beta21, there is a context isolation bypass. Code running in the main wor

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Electronjs	Electron	All	All	All	All
Application	Electronjs	Electron	9.0.0	-	All	All
Application	Electronjs	Electron	9.0.0	beta1	All	All
Application	Electronjs	Electron	9.0.0	beta10	All	All
Application	Electronjs	Electron	9.0.0	beta11	All	All
Application	Electronjs	Electron	9.0.0	beta12	All	All
Application	Electronjs	Electron	9.0.0	beta13	All	All
Application	Electronjs	Electron	9.0.0	beta14	All	All
Application	Electronjs	Electron	9.0.0	beta15	All	All
Application	Electronjs	Electron	9.0.0	beta16	All	All
Application	Electronjs	Electron	9.0.0	beta17	All	All
Application	Electronjs	Electron	9.0.0	beta18	All	All
Application	Electronjs	Electron	9.0.0	beta19	All	All
Application	Electronjs	Electron	9.0.0	beta2	All	All
Application	Electronjs	Electron	9.0.0	beta20	All	All
Application	Electronjs	Electron	9.0.0	beta3	All	All
Application	Electronjs	Electron	9.0.0	beta4	All	All

Application	Electronjs	Electron	9.0.0	beta5	All	All
Application	Electronjs	Electron	9.0.0	beta6	All	All
Application	Electronjs	Electron	9.0.0	beta7	All	All
Application	Electronjs	Electron	9.0.0	beta8	All	All
Application	Electronjs	Electron	9.0.0	beta9	All	All
Application	Electronjs	Electron	All	All	All	All
Application	Electronjs	Electron	9.0.0	-	All	All
Application	Electronjs	Electron	9.0.0	beta1	All	All
Application	Electronjs	Electron	9.0.0	beta10	All	All
Application	Electronjs	Electron	9.0.0	beta11	All	All
Application	Electronjs	Electron	9.0.0	beta12	All	All
Application	Electronjs	Electron	9.0.0	beta13	All	All
Application	Electronjs	Electron	9.0.0	beta14	All	All
Application	Electronjs	Electron	9.0.0	beta15	All	All
Application	Electronjs	Electron	9.0.0	beta16	All	All
Application	Electronjs	Electron	9.0.0	beta17	All	All
Application	Electronjs	Electron	9.0.0	beta18	All	All
Application	Electronjs	Electron	9.0.0	beta19	All	All
Application	Electronjs	Electron	9.0.0	beta2	All	All
Application	Electronjs	Electron	9.0.0	beta20	All	All
Application	Electronjs	Electron	9.0.0	beta3	All	All
Application	Electronjs	Electron	9.0.0	beta4	All	All
Application	Electronjs	Electron	9.0.0	beta5	All	All
Application	Electronjs	Electron	9.0.0	beta6	All	All
Application	Electronjs	Electron	9.0.0	beta7	All	All
Application	Electronjs	Electron	9.0.0	beta8	All	All
Application	Electronjs	Electron	9.0.0	beta9	All	All

References						
Reference				Source	Link	Tags
Stable Releases Electron				MISC	www.electronjs.org	Release Notes, Vendor
Context isolation bypass via contextBridge · Advisory · electron/electron · GitHub				CONFIRM	github.com	Third Party Advisory
CVE Program record				CVE.ORG	www.cve.org	canonical
NVD vulnerability detail				NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[983183](#) Nodejs (npm) Security Update for electron (GHSA-h9jc-284h-533g)

© [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](#)