



CVE-2016-1202

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

Summary

CVE	CVE-2016-1202
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-04-25 18:59:00 UTC
Updated	2016-05-04 22:26:00 UTC
Description	Untrusted search path vulnerability in Atom Electron before 0.33.5 allows local users to gain privileges via a Trojan horse N

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Atom	Electron	All	All	All	All

References

Reference	Source	L
Prevent Node from adding paths outside the app to search paths by zcbenz · Pull Request #2976 · electron/electron · GitHub	CONFIRM	g
Merge pull request #2976 from atom/node_modules_paths · electron/electron@9a2e2b3 · GitHub	CONFIRM	g
JVN#00324715: Electron may insecurely load Node modules	JVN	jv
JVNDB-2016-000054	JVNDB	jv
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

981076 Nodejs (npm) Security Update for electron (GHSA-gvcj-pfq2-wxj7)

© [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](#)