



CVE-2020-5219

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

Summary

CVE	CVE-2020-5219
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-24 16:15:00 UTC
Updated	2020-01-31 20:50:00 UTC
Description	Angular Expressions before version 1.0.1 has a remote code execution vulnerability if you call expressions.compile(userCo

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Peerigon	Angular-expressions	All	All	All	All
Application	Peerigon	Angular-expressions	All	All	All	All

References

Reference	Source	Link
AngularJS: Angular 1.6 - Expression Sandbox Removal	MISC	blog.angularjs.org
Disallow access to prototype chain (CVE-2020-5219) · peerigon/angular-expressions@061addf · GitHub	MISC	github.com
Angular Expressions - Remote Code Execution · Advisory · peerigon/angular-expressions · GitHub	CONFIRM	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: reported by GoSecure Inc

Legacy QID Mappings

[983110](#) Nodejs (npm) Security Update for anular-expressions (GHSA-hxhm-96pp-2m43)

© [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](#)