



CVE-2017-16009

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

Summary

CVE	CVE-2017-16009
State	PUBLIC
Assigner	support@hackerone.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-06-04 19:29:00 UTC
Updated	2023-03-24 18:10:00 UTC
Description	ag-grid is an advanced data grid that is library agnostic. ag-grid is vulnerable to Cross-site Scripting (XSS) via Angular Expr

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ag-grid	Ag-grid	All	All	All	All
Application	Ag-grid	Ag-grid	-	All	All	All
Application	Ag-grid	Ag-grid	-	All	All	All
Application	Angularjs	Angularjs	All	All	All	All
Application	Angularjs	Angularjs	-	All	All	All
Application	Angularjs	Angularjs	-	All	All	All

References

Reference	Source	Link	Tags
[misc] XSS vulnerability: Angular expression injection · Issue #1287 · ag-grid/ag-grid · GitHub	MISC	github.com	Issue Tracking,
AngularJS - Escaping the Expression Sandbox for XSS	MISC	spring.io	Exploit, Techni
Node Security Platform Advisory	MISC	nodesecurity.io	Third Party Adv
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, anal

No vendor comments have been submitted for this CVE.

983005 Nodejs (npm) Security Update for ag-grid (GHSA-wfw3-rgfr-6g67)

© [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](#).

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