



CVE-2019-14863

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-14863
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-02 15:15:00 UTC
Updated	2020-01-09 19:57:00 UTC
Description	There is a vulnerability in all angular versions before 1.5.0-beta.0, where after escaping the context of the web application, t

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Angularjs	Angular.js	All	All	All	All
Application	Redhat	Decision Manager	7.0	All	All	All
Application	Redhat	Decision Manager	7.0	All	All	All
Application	Redhat	Process Automation	7.0	All	All	All
Application	Redhat	Process Automation	7.0	All	All	All

References

Reference	Source
1763589 – (CVE-2019-14863) CVE-2019-14863 angular: Cross-site Scripting (XSS) due to no proper sanitization of xlink:href attributes	CO
Cross-site Scripting (XSS) in angular Snyk	MS
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[981592](#) Nodejs (npm) Security Update for angular (GHSA-r5fx-8r73-v86c)

© [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](#)