



CVE-2019-10785

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

Summary

CVE	CVE-2019-10785
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-13 17:15:00 UTC
Updated	2023-11-07 03:02:00 UTC
Description	dojox is vulnerable to Cross-site Scripting in all versions before version 1.16.1, 1.15.2, 1.14.5, 1.13.6, 1.12.7 and 1.11.9. Th

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Linuxfoundation	Dojox	All	All	All	All
Application	Linuxfoundation	Dojox	All	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 2127-1] dojo security update	MLIST	lists.debian.org	Mailing List, Thi
Page not found Snyk		snyk.io	
XSS due to insufficient escape in dojox.xmpp.util.xmlEncode · Advisory · dojo/dojox · GitHub	MISC	github.com	Exploit, Third P
Invalid vulnerability	MISC	snyk.io	Broken Link
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.

Legacy QID Mappings

© [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](#)