



CVE-2015-5654

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

Summary

CVE	CVE-2015-5654
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-11 01:59:00 UTC
Updated	2016-12-06 03:03:00 UTC
Description	Cross-site scripting (XSS) vulnerability in Dojo Toolkit before 1.2 allows remote attackers to inject arbitrary web script or HT

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dojotoolkit	Dojo	All	All	All	All

References

Reference	Source
JVN#13456571: Dojo Toolkit vulnerable to cross-site scripting	JVN
JVNDB-2015-000153	JVNDB
IBM Security Bulletin: Fix available for Security Vulnerability in IBM WebSphere Portal (CVE-2015-5654) - United States	CONFIRM
Dojo Toolkit CVE-2015-5654 Unspecified Cross Site Scripting Vulnerability	BID
IBM WebSphere Portal Input Validation Flaw in Dojo Toolkit Lets Remote Conduct Cross-Site Scripting Attacks - SecurityTracker	SECTRAC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980650 Nodejs (npm) Security Update for dojo (GHSA-p82g-2xpp-m5r3)

© [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](#)