



CVE-2015-9286

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2015-9286
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-04-30 14:29:00 UTC
Updated	2019-05-01 14:22:00 UTC
Description	Controllers.outgoing in controllers/index.js in NodeBB before 0.7.3 has outgoing XSS.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nodebb	Nodebb	All	All	All	All
Application	Nodebb	Nodebb	All	All	All	All

References

Reference	Source	Link
Update index.js, fix outgoing XSS by mikicaivosevic · Pull Request #3371 · NodeBB/NodeBB · GitHub	MISC	github.com
Comparing 56b79a9...4de7529 · NodeBB/NodeBB · GitHub	MISC	github.com
www.vulnerability-lab.com/get_content.php	MISC	www.vulnerability-lab.co
NodeBB v0.8.2 - Client Side Cross Site Web Vulnerability	MISC	vulners.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

981799 Nodejs (npm) Security Update for nodebb (GHSA-72fv-qgj6-2w2p)

© [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](#)