



CVE-2018-15917

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

Summary

CVE	CVE-2018-15917
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-09-05 21:29:00 UTC
Updated	2022-07-05 15:12:00 UTC
Description	Persistent cross-site scripting (XSS) issues in Jorani 0.6.5 allow remote attackers to inject arbitrary web script or HTML via

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Jorani	Jorani	0.6.5	All	All	All
Application	Jorani	Jorani	0.6.5	All	All	All
Application	Jorani Project	Jorani	0.6.5	All	All	All

References

Reference	Source	Link
Jorani Leave Management 0.6.5 - Cross-Site Scripting - PHP webapps Exploit	EXPLOIT-DB	www.exploit-db.com
CVE-2018-15917 Jorani Leave Management System 0.6.5 - Cross-Site Scripting Persistente - Hackpuntos	MISC	hackpuntos.com
Multiple Vulnerabilities · Issue #254 · bbalet/jorani · GitHub	MISC	github.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.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)