



CVE-2017-6478

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

Summary

CVE	CVE-2017-6478
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-05 20:59:00 UTC
Updated	2021-01-08 13:54:00 UTC
Description	paintballrefjosh/MaNGOSWebV4 before 4.0.8 is vulnerable to a reflected XSS in install/index.php (step parameter).

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mangoswebv4 Project	Mangoswebv4	All	All	All	All
Application	Mangoswebv4 Project	Mangoswebv4	All	All	All	All

References

Reference	Source	Link
I have find a Reflected XSS vulnerability in this project · Issue #15 · paintballrefjosh/MaNGOSWebV4 · GitHub	CONFIRM	github.com
Release Version 4.0.8 - Added new templates, fixed XSS exploit · paintballrefjosh/MaNGOSWebV4 · GitHub	CONFIRM	github.com
MaNGOSWebV4 CVE-2017-6478 Cross Site Scripting Vulnerability	BID	www.securityfocus.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.

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