



WordPress adivaha Travel Plugin 2.3 Reflected XSS via isMobile

MITRE

NVD

CVE.ORG

JSON API

Print: PDF

Summary	
CVE	CVE-2023-54358
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-09 21:16:04 UTC
Updated	2026-04-13 15:02:27 UTC
Description	WordPress adivaha Travel Plugin 2.3 contains a reflected cross-site scripting vulnerability that allows unauthenticated attac

Risk And Classification

Primary CVSS: v4.0 5.1 MEDIUM from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:~X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.000820000 probability, percentile 0.240170000 (date 2026-04-15)

Problem Types: CWE-79 | CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA
4.0	CNA	CVSS	5.1	MEDIUM	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA
3.1	disclosure@vulncheck.com	Primary	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
3.1	CNA	CVSS	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVSS v4.0 Breakdown	
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	

None

User Interaction

Active

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

Low

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX:MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Adivaha	WordPress Adivaha Travel Plugin	affected 2.3	Not specified

References

Reference	Source	Link	Ti
www.exploit-db.com/exploits/51663	disclosure@vulncheck.com	www.exploit-db.com	
wordpress.org/plugins/adiaha-hotel	disclosure@vulncheck.com	wordpress.org	
www.ativaha.com	disclosure@vulncheck.com	www.ativaha.com	
www.vulncheck.com/advisories/wordpress-ativaha-travel-plugin-reflected-xss-via-...	disclosure@vulncheck.com	www.vulncheck.com	
CVE Program record	CVE.ORG	www.cve.org	C&
NVD vulnerability detail	NVD	nvd.nist.gov	C&

Vendor Comments And Credit

Discovery Credit

CNA: CraCkEr (en)

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