Microsoft Clarity <= 0.9.3 - Cross-Site Request Forgery to Stored Cross-Site Scripting

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2024-0590
State	PUBLISHED
Assigner	Wordfence
Source Priority	CVE Program / NVD first with legacy fallback
Published	2024-02-29 01:43:22 UTC
Updated	2026-04-08 19:19:12 UTC
Description	The Microsoft Clarity plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including,

Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from nvd@nist.gov

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

EPSS: 0.247560000 probability, percentile 0.961650000 (date 2026-04-22)

Problem Types: CWE-352 | CWE-352 CWE-352 Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	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	security@wordfence.com	Secondary	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	DECLARED	6.1	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

ntegrity

Low

vailability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Clarity	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Microsoft	Microsoft Clarity	affected 0.9.3 semver	Not specified

References

Reference	Source	Link
www.wordfence.com/threat-intel/vulnerabilities/id/c2f4461b-1373-4d09-8430-14d19...	af854a3a-2127-422b-91ae-364da2661108	www.wo
plugins.trac.wordpress.org/changeset	af854a3a-2127-422b-91ae-364da2661108	plugins.t
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.

Vendor Comments And Credit

Discovery Credit

CNA: GiongfNef (en)

CNA: Kodai Kubono (en)

Additional Advisory Data

Source	Time	Event
CNA	2024-02-16T00:00:00.000Z	Disclosed

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report