



WordPress Cookies and Content Security Policy Plugin

<= 2.15 is vulnerable to Sensitive Data Exposure

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

Summary	
CVE	CVE-2023-40662
State	PUBLISHED
Assigner	Patchstack
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-11-30 15:15:08 UTC
Updated	2026-04-28 19:21:12 UTC
Description	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Jonk @ Follow me Darling Cookies and Content

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from nvd@nist.gov

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

Problem Types: CWE-200 | NVD-CWE-noinfo | CWE-200 CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	audit@patchstack.com	Secondary	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
3.1	CNA	CVSS	5.3	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v3.1 Breakdown	
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality	High

High

Integrity

None

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Followmedarling	Cookies And Content Security Policy	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Jonk @ Follow Me Darling	Cookies And Content Security Policy	affected n/a 2.15 custom	Not specified

References

Reference	Source
WordPress Cookies and Content Security Policy plugin <= 2.15 - Sensitive Data Exposure vulnerability - Patchstack	af854a3a-2127-422b-9
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Mika (Patchstack Alliance) (en)

Additional Advisory Data

Solutions

CNA: Update to 2.16 or a higher version.

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