



# WP Reset <= 2.0 - Sensitive Information Exposure due to Insufficient Randomness

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

## Summary

<b>CVE</b>	CVE-2023-6799
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-04-09 19:15:12 UTC
<b>Updated</b>	2026-04-08 18:18:41 UTC
<b>Description</b>	The WP Reset – Most Advanced WordPress Reset Tool plugin for WordPress is vulnerable to Sensitive Information Exposure

## Risk And Classification

**Primary CVSS:** v3.1 5.9 MEDIUM from nvd@nist.gov

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

**Problem Types:** CWE-330 | CWE-330 CWE-330 Use of Insufficiently Random Values

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	security@wordfence.com	Secondary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
3.1	CNA	DECLARED	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

None

Availability

None

CVSS:3.1/AV:N/AC:H/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	WebfactoryLtd	Wp Reset	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Webfactory	WP Reset	affected 2.0 semver	Not specified

### References

Reference	Source	Link
plugins.trac.wordpress.org/changeset	af854a3a-2127-422b-91ae-364da2661108	plugins.t
www.wordfence.com/threat-intel/vulnerabilities/id/68f41e88-ed36-4361-bddd-41495...	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:** Justin Kennedy (en)

### Additional Advisory Data

Source	Time	Event
CNA	2024-03-26T00:00:00.000Z	Disclosed

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)