



# Maintenance Mode <= 3.0.1 - Information Exposure

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2024-1478
<b>State</b>	PUBLISHED
<b>Assigner</b>	Wordfence
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2024-03-05 02:15:26 UTC
<b>Updated</b>	2026-04-08 18:20:40 UTC
<b>Description</b>	The Maintenance Mode plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and incl

## Risk And Classification

**Primary CVSS:** v3.1 5.3 MEDIUM from security@wordfence.com

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

**Problem Types:** CWE-284 | NVD-CWE-noinfo | CWE-284 CWE-284 Improper Access Control

Version	Source	Type	Score	Severity	Vector
3.1	security@wordfence.com	Secondary	5.3	MEDIUM	<b>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N</b>
3.1	CNA	DECLARED	5.3	MEDIUM	<b>CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N</b>

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**None**

User Interaction

**None**

Scope

**Unchanged**

Confidentiality

**Low**

Integrity

**None**

Availability

None

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

#### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Helderk	Maintenance Mode	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Helderk	Maintenance Mode	affected 3.0.1 semver	Not specified
ADP	Helderk	Maintenance Mode	affected 2.5.0 semver	Not specified

#### References

Reference	Source	Link
wordpress.org/plugins/hkdev-maintenance-mode	af854a3a-2127-422b-91ae-364da2661108	wordpres
plugins.trac.wordpress.org/changeset	security@wordfence.com	plugins.tr
www.wordfence.com/threat-intel/vulnerabilities/id/36def628-e09e-4da0-ab14-35aef...	af854a3a-2127-422b-91ae-364da2661108	www.wor
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.g

#### Vendor Comments And Credit

Discovery Credit

**CNA:** Francesco Carlucci (en)

#### Additional Advisory Data

Source	Time	Event
CNA	2024-03-04T00:00:00.000Z	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)