



# CVE-2020-36730

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2020-36730
<b>State</b>	PUBLIC
<b>Assigner</b>	security@wordfence.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-06-07 02:15:00 UTC
<b>Updated</b>	2023-11-07 03:22:00 UTC
<b>Description</b>	The CMP for WordPress is vulnerable to authorization bypass due to a missing capability check on the cmp_get_post_data

## Risk And Classification

**Problem Types:** CWE-862

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Niteothemes	Cmp	All	All	All	All

## References

Reference	Source	Link
WordPress Plugin CMP-Coming Soon & Maintenance by NiteoThemes Security Bypass (3.8.1) - Vulnerabilities - Acunetix	MISC	<a href="#">www</a>
Just a moment...	MISC	<a href="#">wps</a>
Multiple vulnerabilities fixed in CMP – Coming Soon and Maintenance plugin. – NinTechNet	MISC	<a href="#">blog</a>
CMP <= 3.8.1 - Missing Authorization	MISC	<a href="#">www</a>
CVE Program record	CVE.ORG	<a href="#">www</a>
NVD vulnerability detail	NVD	<a href="#">nvd</a>

No vendor comments have been submitted for this CVE.

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

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](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**