



# CVE-2021-24240

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

## Summary

<b>CVE</b>	CVE-2021-24240
<b>State</b>	PUBLIC
<b>Assigner</b>	contact@wpscan.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2021-04-22 21:15:00 UTC
<b>Updated</b>	2021-04-29 20:50:00 UTC
<b>Description</b>	The Business Hours Pro WordPress plugin through 5.5.0 allows a remote attacker to upload arbitrary files using its manual

## Risk And Classification

**Problem Types:** CWE-434

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Aivahthemes	Business Hours Pro	All	All	All	All

## References

Reference	Source	Link	Tags
Business Hours Pro WordPress Plugin by AivahThemes   CodeCanyon	MISC	<a href="https://www.codecanyon.net">codecanyon.net</a>	
Business Hours Pro <= 5.5.0 - Unauthenticated Arbitrary File Upload to RCE Security Vulnerability	CONFIRM	<a href="https://wpscan.com">wpscan.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Harald Eilertsen

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](#).

**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)