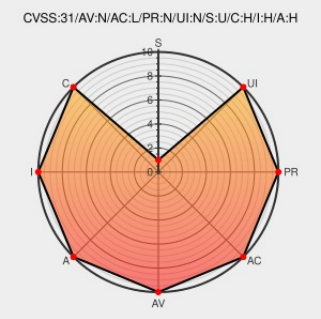
CVE-2021-28428

Published on: Not Yet Published

Last Modified on: 04/15/2022 08:16:00 PM UTC

CVE-2021-28428

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Horizontcms from Horizontcms Project contain the following vulnerability:

File upload vulnerability in HorizontCMS before 1.0.0-beta.3 via uploading a .htaccess and *.hello files using the Media Files upload functionality. The original file upload vulnerability (CVE-2020-27387) was remediated by restricting the PHP extensions; however, we confirmed that the filter was bypassed via uploading an arbitrary .htaccess and *.hello files in order to execute PHP code to gain RCE.

CVE-2021-28428 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
GitHub - ttimot24/HorizontCMS: Lightweight CMS built on Laravel	github.com text/html	MISC github.com/ttimot24/HorizontCMS

8, VueJs 2.6 and Bootstrap 3.4.3/4.5.3.		
#30 - Security fix: File extension bypass · ttimot24/HorizontCMS@9c4d682 · GitHub	github.com text/html	MISC github.com/ttimot24/HorizontCMS/commit/9c4d6827cbe96dececc6834d53660e14ab2bf8838

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Horizontcms Project	Horizontcms	1.0.0	-	All	All
Application	Horizontcms Project	Horizontcms	1.0.0	alpha	All	All
Application	Horizontcms Project	Horizontcms	1.0.0	alpha2	All	All
Application	Horizontcms Project	Horizontcms	1.0.0	alpha3	All	All
Application	Horizontcms Project	Horizontcms	1.0.0	alpha4	All	All
Application	Horizontcms Project	Horizontcms	1.0.0	alpha5	All	All
Application	Horizontcms Project	Horizontcms	1.0.0	alpha6	All	All
Application	Horizontcms Project	Horizontcms	1.0.0	alpha7	All	All
Application	Horizontcms Project	Horizontcms	1.0.0	alpha8	All	All
Application	Horizontcms Project	Horizontcms	1.0.0	beta	All	All
Application	Horizontcms Project	Horizontcms	1.0.0	beta2	All	All

cpe:2.3:a:horizontcms_project:horizontcms:1.0.0:-:*:*:*:*:*:*:

cpe:2.3:a:horizontcms_project:horizontcms:1.0.0:alpha:*:*:*:*:*:*:

cpe:2.3:a:horizontcms_project:horizontcms:1.0.0:alpha2:*:*:*:*:*:*:

cpe:2.3:a:horizontcms_project:horizontcms:1.0.0:alpha3:*:*:*:*:*:*:

cpe:2.3:a:horizontcms_project:horizontcms:1.0.0:alpha4:*:*:*:*:*:*:

cpe:2.3:a:horizontcms_project:horizontcms:1.0.0:alpha5:*:*:*:*:*:*:

cpe:2.3:a:horizontcms_project:horizontcms:1.0.0:alpha6:*:*:*:*:*:*:

cpe:2.3:a:horizontcms_project:horizontcms:1.0.0:alpha7:*:*:*:*:*:*:

cpe:2.3:a:horizontcms_project:horizontcms:1.0.0:alpha8:*:*:*:*:*:*:

cpe:2.3:a:horizontcms_project:horizontcms:1.0.0:beta:*:*:*:*:*:*:

cpe:2.3:a:horizontcms_project:horizontcms:1.0.0:beta2:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-28428 : File upload vulnerability in HorizontCMS before 1.0.0-beta.3 via uploading a .htaccess and *.hello… twitter.com/i/web/status/1…	2022-04-05 16:08:49
@WesUncensored	New vulnerability on the NVD: CVE-2021-28428 ift.tt/EjrLfcG	2022-04-05 18:33:31
@workentin	New vulnerability on the NVD: CVE-2021-28428 ift.tt/EjrLfcG	2022-04-05 18:40:08
/r/netcve	CVE-2021-28428	2022-04-05 17:38:56

← Previous ID

Next ID→