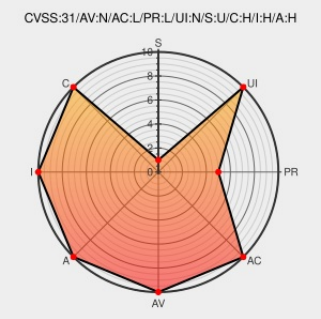
CVE-2020-27387

Published on: 11/04/2020 12:00:00 AM UTC

Last Modified on: 10/19/2022 03:58:00 PM UTC

CVE-2020-27387

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



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

An unrestricted file upload issue in HorizontCMS through 1.0.0-beta allows an authenticated remote attacker (with access to the FileManager) to upload and execute arbitrary PHP code by uploading a PHP payload, and then using the FileManager's rename function to provide the payload (which will receive a random name on the server) with the PHP extension, and finally executing the PHP file via an HTTP GET request to /storage/<php_file_name>. NOTE: the vendor has patched this while leaving the version number at 1.0.0-beta.

CVE-2020-27387 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link

What's in a name: RCE Hunting in CMSs via Unrestricted File Upload	blog.vonahi.io text/html	MISC blog.vonahi.io/whats-in-a-re-name/
Add HorizontCMS 1.0.0-beta exploit module and documentation by kalba-security · Pull Request #14340 · rapid7/metasploit-framework · GitHub	Third Party Advisory github.com text/html	MISC github.com/rapid7/metasploit-framework/pull/14340
Security bug fix. · ttimot24/HorizontCMS@436b5ab · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/ttimot24/HorizontCMS/commit/436b5ab679fd27afa3d99c023dbe103
HorizontCMS 1.0.0-beta Shell Upload ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/160046/HorizontCMS-1.0.0-beta-Shell-Upload.html

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	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	All	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

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:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Php - CVE-2020-27387: github.com/rapid7/metaspl…	2022-10-19 17:03:28

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report