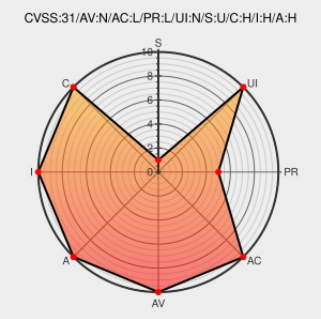
CVE-2018-6383

Published on: 01/29/2018 12:00:00 AM UTC

Last Modified on: 02/10/2022 07:23:00 AM UTC

CVE-2018-6383

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



Certain versions of Monstra from Monstra contain the following vulnerability:

Monstra CMS through 3.0.4 has an incomplete "forbidden types" list that excludes .php (and similar) file extensions but not the .pht or .phar extension, which allows remote authenticated Admins or Editors to execute arbitrary PHP code by uploading a file, a different vulnerability than CVE-2017-18048.

CVE-2018-6383 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
Exploits/CVE-2018-6383-Exploit at main · Hacker5preme/Exploits · GitHub	github.com text/html	MISC github.com/Hacker5preme/Exploits/tree/main/CVE-2018-6383-Exploit

Monstra CMS 3.0.4 Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/162968/Monstra-CMS-3.0.4-Remote-Code-Execution.html
Some extension can bypassed extension filter in uploading process · Issue #429 · monstra-cms/monstra · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/monstra-cms/monstra/issues/429

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Monstra	Monstra	All	All	All	All

cpe:2.3:a:monstra:monstra:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→