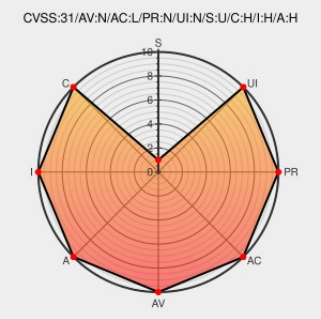
CVE-2018-16763

Published on: 09/09/2018 12:00:00 AM UTC

Last Modified on: 11/30/2021 10:07:00 PM UTC

CVE-2018-16763

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



Certain versions of Fuel Cms from Thedaylightstudio contain the following vulnerability:

FUEL CMS 1.4.1 allows PHP Code Evaluation via the pages/select/ filter parameter or the preview/ data parameter. This can lead to Pre-Auth Remote Code Execution.

CVE-2018-16763 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
fuelCMS 1.4.1 Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/153696/fuelCMS-1.4.1-Remote-Code-Execution.html
fuelCMS 1.4.1 - Remote Code Execution - Linux webapps Exploit	www.exploit-db.com Proof of Concept	EXPLOIT-DB 47138

	text/html	
Fuel CMS 1.4.1 Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/164756/Fuel-CMS-1.4.1-Remote-Code-Execution.html
From Code Evaluation to Pre-Auth Remote Code Execution (CVE-2018-16763 bypass) – 0xD0ff9	0xd0ff9.wordpress.com text/html	MISC 0xd0ff9.wordpress.com/2019/07/19/from-code-evaluation-to-pre-auth-remote-code-execution-cve-2018-16763-bypass/
Fuel CMS 1.4 Remote Code Execution ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/160080/Fuel-CMS-1.4-Remote-Code-Execution.html
Vulnerability - Code Evaluations & SQL Injections · Issue #478 · daylightstudio/FUEL-CMS · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/daylightstudio/FUEL-CMS/issues/478

There are currently no QIDs associated with this CVE

Exploit/POC from Github

CVE 2018-16763

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Thedaylightstudio	Fuel Cms	All	All	All	All

cpe:2.3:a:thedaylightstudio:fuel_cms:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/LiveOverflow	Exploiting Fuel CMS CVE-2018-16763 | TryHackMe Ignite	2021-03-02 10:59:17
/r/netsecstudents	Exploiting Fuel CMS CVE-2018-16763 | TryHackMe Ignite	2021-03-02 09:09:43
/r/oscp	Exploiting Fuel CMS CVE-2018-16763 | TryHackMe Ignite	2021-03-02 09:07:14
/r/Hacking_Tutorials	Exploiting Fuel CMS CVE-2018-16763 | TryHackMe Ignite	2021-03-02 09:05:22

← Previous ID

Next ID→

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