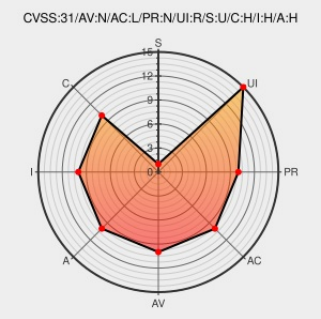
CVE-2020-7991

Published on: 01/26/2020 12:00:00 AM UTC

Last Modified on: 01/31/2023 09:04:00 PM UTC

CVE-2020-7991

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



Certain versions of Framework from Adive contain the following vulnerability:

Adive Framework 2.0.8 has admin/config CSRF to change the Administrator password.

CVE-2020-7991 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	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
Adive Framework 2.0.8 - Persistent Cross-Site Scripting - PHP webapps Exploit	Exploit, Third Party Advisory, VDB Entry, www.exploit-db.com, Proof of Concept	MISC www.exploit-db.com/exploits/47946

	text/html	
adive-php7/README.md at master · ferdinandmartin/adive-php7 · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/ferdinandmartin/adive-php7/blob/master/README.md
Adive Framework 2.0.8 Cross Site Request Forgery ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/156106/Adive-Framework-2.0.8-Cross-Site-Request-Forgery.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adive	Framework	2.0.8	All	All	All
Application	Adive	Framework	2.0.8	All	All	All

cpe:2.3:a:adive:framework:2.0.8:*:*:*:*:*:*:*:

cpe:2.3:a:adive:framework:2.0.8:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@hardikkp95	DAY 5 Out 100 Days Cyberlearning CVE-2020-15038 CVE-2020-7991 CVE-2020-8547 CVE-2020-9043 MALWARE ANALYSIS - VBSc… twitter.com/i/web/status/1…	2021-12-26 18:16:00

← Previous ID

Next ID→