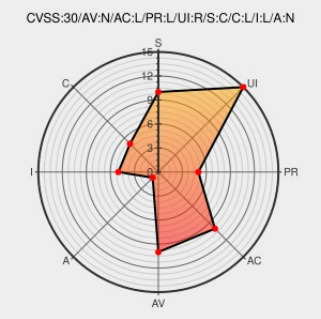
CVE-2018-9120

Published on: 03/29/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:55 PM UTC

CVE-2018-9120

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



Certain versions of Crea8social from Crea8social contain the following vulnerability:

In Crea8social 2018.2, there is Stored Cross-Site Scripting via a post.

CVE-2018-9120 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
- YouTube	Exploit Third Party Advisory www.youtube.com text/html	MISC www.youtube.com/watch?v=QqJFh3Ame9g

Multiple Cross-Site Scripting Vulnerabilities in Crea8Social Social Network Script – Seekurity	Exploit Technical Description Third Party Advisory www.seekurity.com text/html	MISC www.seekurity.com/blog/general/multiple-cross-site-scripting-vulnerabilities-in-crea8social-social-network-script/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Crea8social	Crea8social	2018.2	All	All	All
Application	Crea8social	Crea8social	2018.2	All	All	All

cpe:2.3:a:crea8social:crea8social:2018.2:*:*:*:*:*:*:*

cpe:2.3:a:crea8social:crea8social:2018.2:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→