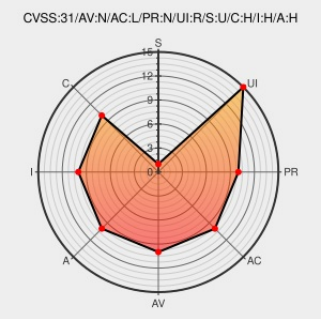
CVE-2020-11610

Published on: 04/07/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-11610

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



Certain versions of Cross Domain Local Storage from Cross Domain Local Storage Project contain the following vulnerability:

An issue was discovered in xdLocalStorage through 2.0.5. The postData() function in xdLocalStoragePostMessageApi.js specifies the wildcard (*) as the targetOrigin when calling the postMessage() function on the parent object. Therefore any domain can load the application hosting the "magical iframe" and receive the messages that the "magical iframe" sends.

CVE-2020-11610 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
GitHub - ofirdagan/cross-domain-local-storage: A neet solution for cross domain local storage using invisible iframe and post	Product github.com	MISC github.com/ofirdagan/cross-domain-local-storage

messages	text/html	
Exploiting xdLocalStorage (localStorage and postMessage) – GrimBlog	Exploit Third Party Advisory grimhacker.com text/html	MISC grimhacker.com/exploiting-xdlocalstorage-localstorage-and-postmessage/#Missing-TargetOrigin-Magic-iframe

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cross Domain Local Storage Project	Cross Domain Local Storage	All	All	All	All

cpe:2.3:a:cross_domain_local_storage_project:cross_domain_local_storage:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→