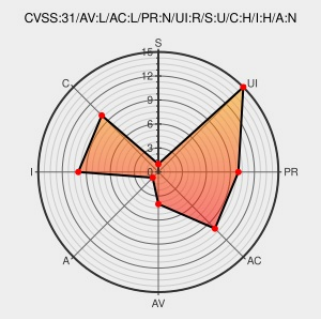
CVE-2015-9545

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

Last Modified on: 03/23/2021 11:26:21 PM UTC

CVE-2015-9545

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 receiveMessage() function in xdLocalStorage.js does not implement any validation of the origin of web messages. Remote attackers who can entice a user to load a malicious site can exploit this issue to impact the confidentiality and integrity of data in the local storage of the vulnerable site via malicious web messages.

CVE-2015-9545 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.1 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	NONE

CVSS2 Score: 5.8 - MEDIUM

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

CVE References

Description	Tags	Link
Whitelist origin & Ng waitForApi fix by Hengjie · Pull Request #19 · ofirdagan/cross-domain-local-storage · GitHub	Patch, Third Party Advisory	MISC github.com/ofirdagan/cross-domain-local-storage/pull/19

	github.com text/html	
GitHub - ofirdagan/cross-domain-local-storage: A neet solution for cross domain local storage using invisible iframe and post messages	Product Third Party Advisory github.com text/html	MISC github.com/ofirdagan/cross-domain-local-storage
Restricting domain by origins · Issue #17 · ofirdagan/cross-domain-local-storage · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/ofirdagan/cross-domain-local-storage/issues/17
Exploiting xdLocalStorage (localStorage and postMessage) – GrimBlog	Exploit Third Party Advisory grimhacker.com text/html	MISC grimhacker.com/exploiting-xdlocalstorage-localstorage-and-postmessage/#Missing-Origin-Client

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→