

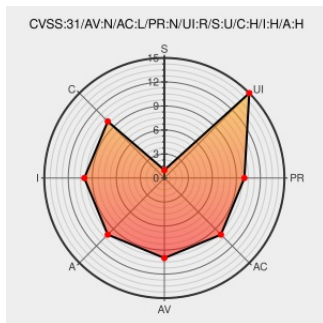


CVE-2020-11610

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 [M](#) 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 neat solution for cross domain local storage using invisible iframe and post	Product github.com	MISC github.com/ofirdagan/cross-domain-local-storage

text/html

text/html

MISC grimhacker.com/exploiting-

comment@cve.report

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

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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