ifmacedo Update IDCE-SQLi History

1 contributor

45 lines (34 sloc) | 2.01 KB

```
1  Presentation:
2  Security vulnerability: SQL Injection.
3  Vulnerability Type: Injections.
4  Affected Component: Affected function on database access code.
5  Software: IDCE MV.
6  Version: 1.0 (discontinued).
7  Bussiness area: Health, Medicine.
8
9  Describe the bug/issue:
10 SQL injection in Logon Page of IDCE MV's application, version 1.0, allows an attacker to inject SQ
11 to access private and sensitive information.
12
13 Have you searched the internet or Github for an answer?
14 Yes.
15
16 To Reproduce:
17 The SQL Injection running over a Time-Based Blind technique.
18 The database usually is an Oracle, but it could be changed.
19
20 1. Open the IDCE's login page. Fill in the user and password fields and intercept it with Burp Sui
21 2. Copy the request lines in the Burp Suite and paste the lines into a new file. Rename this file
22 3. Now, into the "idce-sqli.txt" file, edit the last line. Find the "txtUsuario=" and change it to
23 4. Save the file "idce-sqli.txt".
24 5. Execute SQLMap with the following command: sqlmap -r idce-sqli.txt --dbms=oracle --level=5 --ri
25 6. Wait for the end of SQLi execution.
26
27 DBMS of this application usually is an Oracle, but you could have to find out the DBMS whether it
28 sqlmap -r idce-sqli.txt --dbs --level=5 --risk=3 --technique=T
29
```

```
If you do not have success with the Time-Based techniques, try out all other possible techquines w
sqlmap -r idce-sqli.txt --dbs --level=5 --risk=3

All database's information will be disclosed. But if you have used Time-Based Blind technique, it
So, be patient.

Expected behavior:
Parameterized SQL queries.

Bug Fix:
Update to the latest version.

Additional context:
The procedure is to request a new CVE identifier when an vulnerability was previously considered f

CVE ID: CVE-2022-30496
```