CandidATS 3.0.0 - CSRF to Privilege Escalation

Summary

Affected versions	Version 3.0.0
State	Public
Release date	2022-10-27

Vulnerability

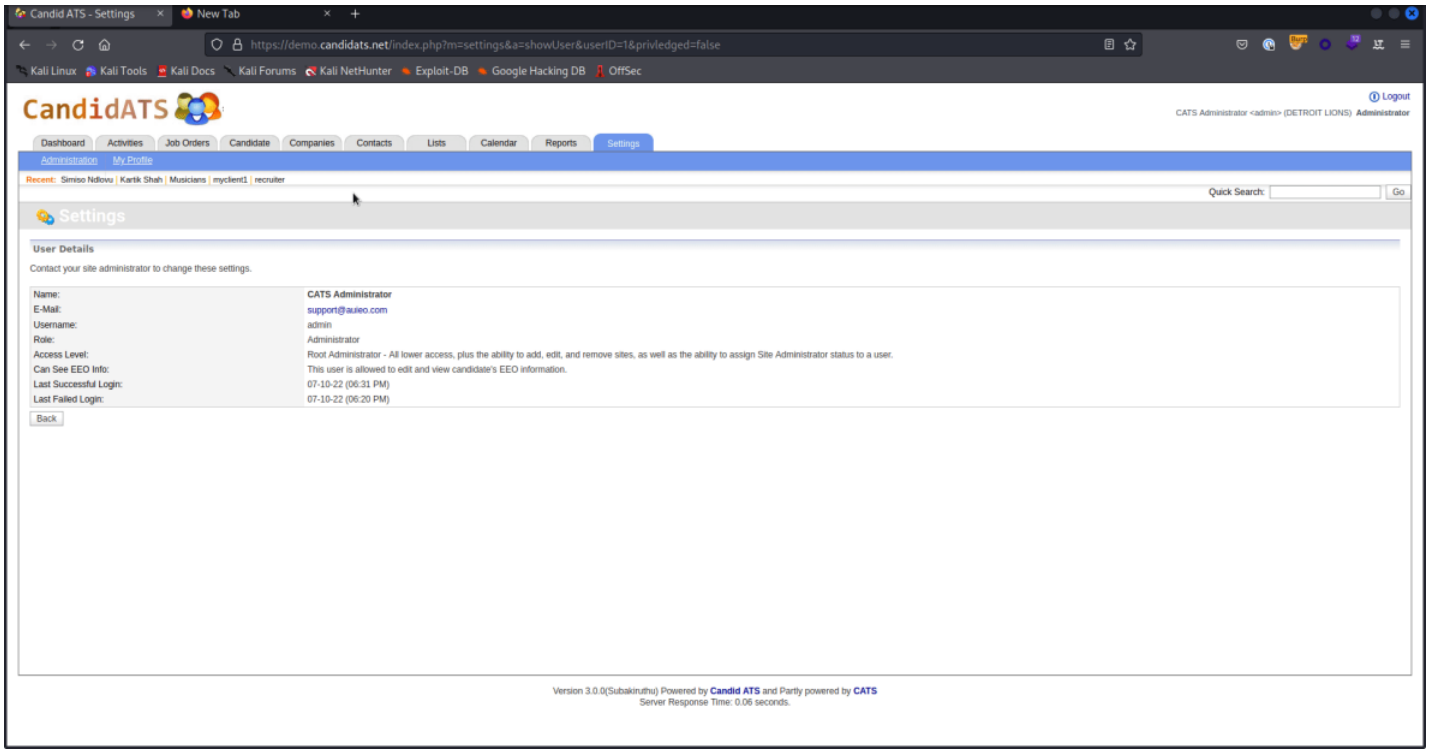
Kind	Cross-site request forgery
Rule	007. Cross-site request forgery
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVSSv3 Base Score	8.8
Exploit available	Yes
CVE ID(s)	CVE-2022-42751

Vulnerability

The stored XSS present in CandidATS 3.0.0 allows a remote attacker to elevate privileges in the application. To trigger this vulnerability, we will need to persuade an administrator to open a malicious link.

Exploitation

In this attack we will elevate privileges in the application, through a malicious link.



Our security policy

- Version: CandidATS 3.0.0
- Operating System: GNU/Linux

Mitigation

There is currently no patch available for this vulnerability.

Credits

The vulnerability was discovered by Carlos Bello from Fluid Attacks' Offensive Team.

References

Vendor page https://candidats.net/

Timeline

- 2022-10-07
  Vulnerability discovered.
- 2022-10-07
  Vendor contacted.
- 2022-10-07
  Vendor replied acknowledging the report.
- 2022-10-27
  Public Disclosure.

Services

Continuous Hacking

One-shot Hacking

Comparative

Solutions

DevSecOps

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

Documentation

Contact