



attacks

[Home](#) / [Advisories](#) / [CandidATS 3.0.0 CSRF to Privilege Escalation](#)

CandidATS 3.0.0 – CSRF to Privilege Escalation

Summary



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](#)

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

Vulnerability

Kind	Cross-site request forgery
Rule	<u>007. Cross-site request forgery</u>
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)	<u>CVE-2022-42751</u>



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

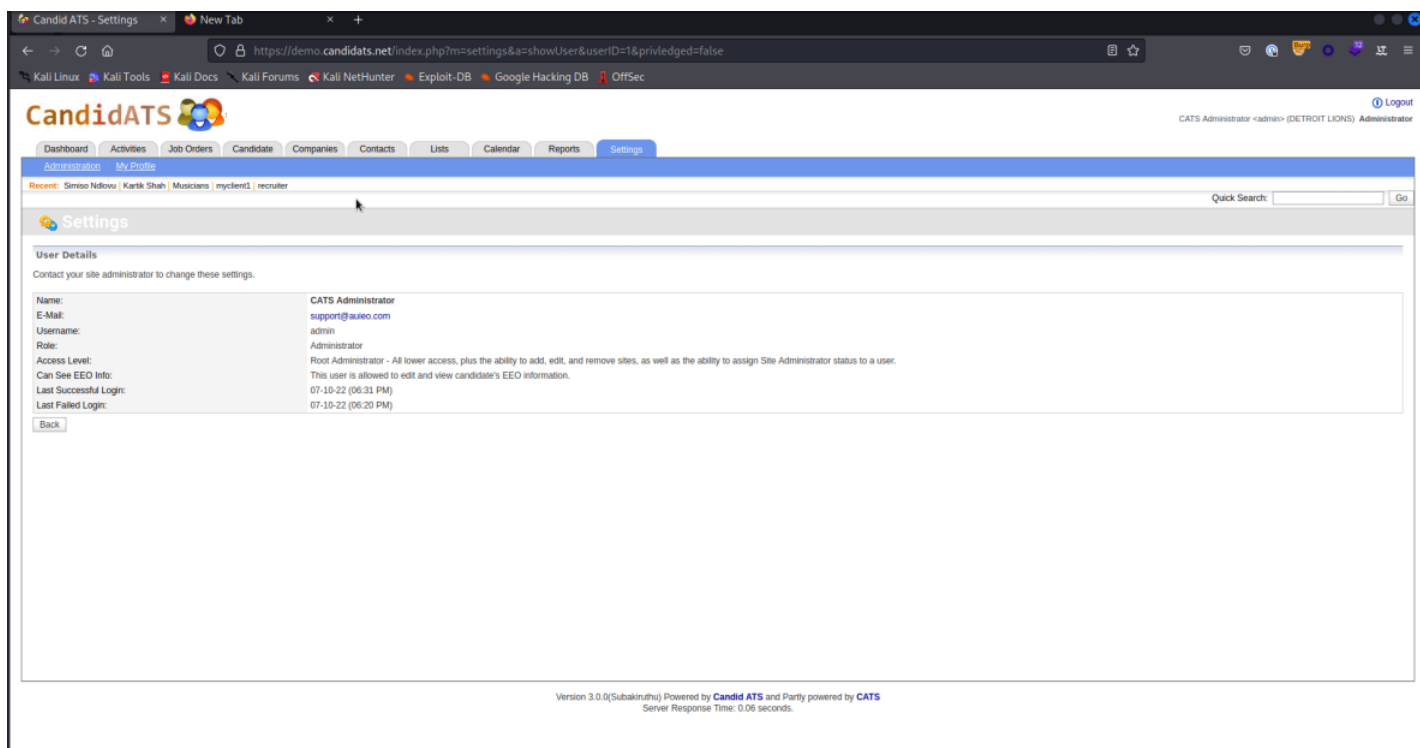
Show details

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



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](#)

- 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.



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



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



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](#)

Documentation

Contact

Copyright © 2022 Fluid Attacks. We hack your software. All rights reserved.

[Service Status](#) - [Terms of Use](#) - [Privacy Policy](#) - [Cookie Policy](#)