



## CandidATS 3.0.0 – Stored XSS to Account Takeover

### 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](#)

<b>Affected versions</b>	Version 3.0.0
<b>State</b>	Public
<b>Release date</b>	2022-10-27

### Vulnerability

<b>Kind</b>	Stored cross-site scripting (XSS)
<b>Rule</b>	<u>083. Stored cross-site scripting (XSS)</u>
<b>Remote</b>	Yes
<b>CVSSv3 Vector</b>	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
<b>CVSSv3 Base Score</b>	8.8
<b>Exploit available</b>	Yes
<b>CVE ID(s)</b>	<u>CVE-2022-42750</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](#)

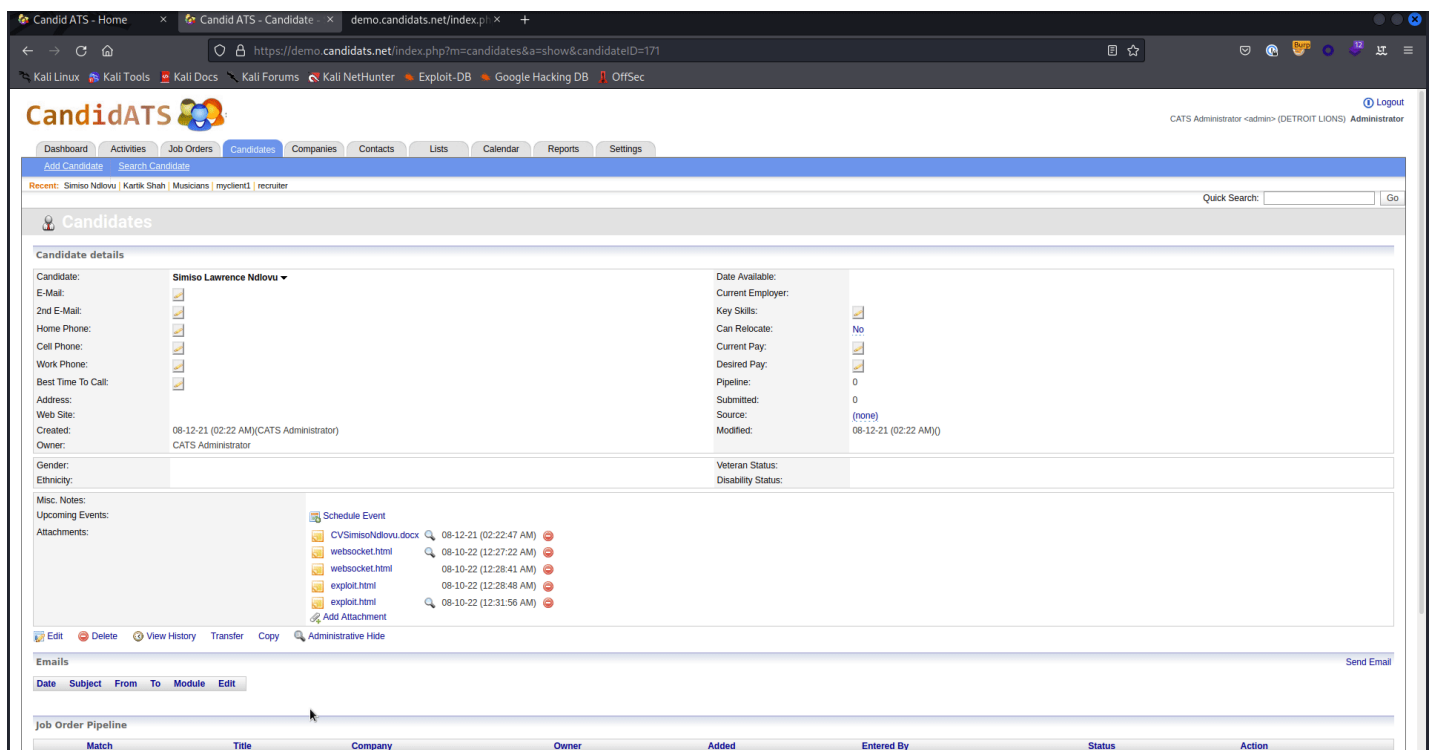
[Show details](#)

## Vulnerability

The Stored XSS present in CandidATS 3.0.0 allows an unauthenticated remote attacker to perform an Account Takeover. To trigger this vulnerability, we will need to force a user to upload a malicious file and wait for them to view the file.

## Exploitation

In this attack we will obtain the administrator user account, through a malicious link.



## 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

OK

## Our security policy

We have reserved the CVE-2022-42750 to refer to these issues from now on.

- <https://fluidattacks.com/advisories/policy/>

## System Information

- 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/>



### 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](#)



Vendor contacted.



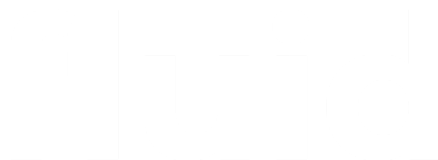
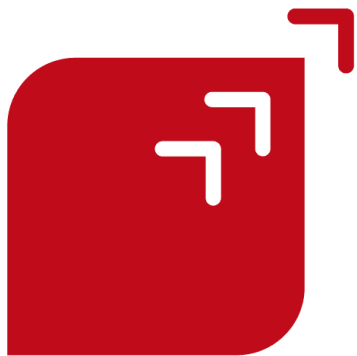
2022-10-07

Vendor replied acknowledging the report.



2022-10-27

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](#)

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

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

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