CandidATS 3.0.0 - Stored XSS to Account Takeover

Summary

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

Vulnerability

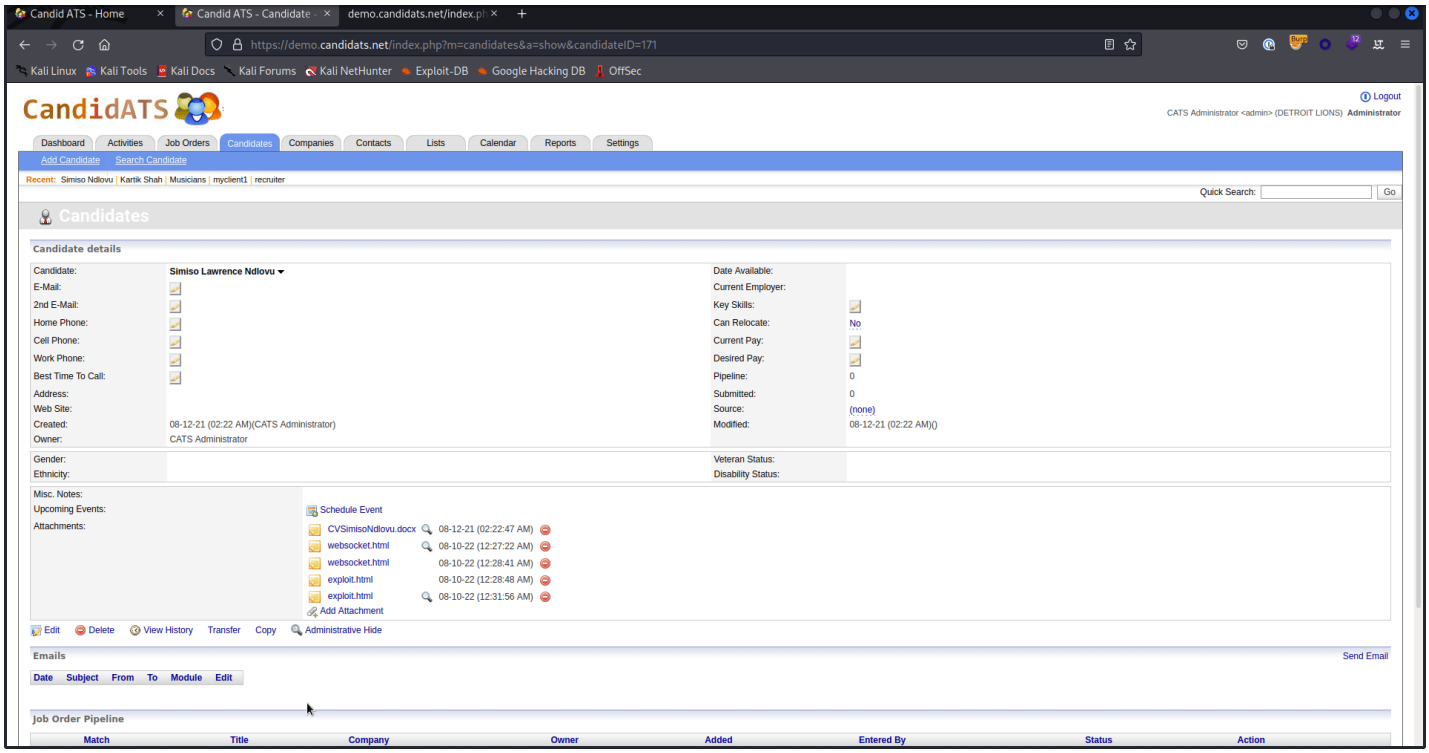
Kind	Stored cross-site scripting (XSS)
Rule	083. Stored cross-site scripting (XSS)
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVSSv3 Base Score	8.8
Exploit available	Yes
CVE ID(s)	CVE-2022-42750

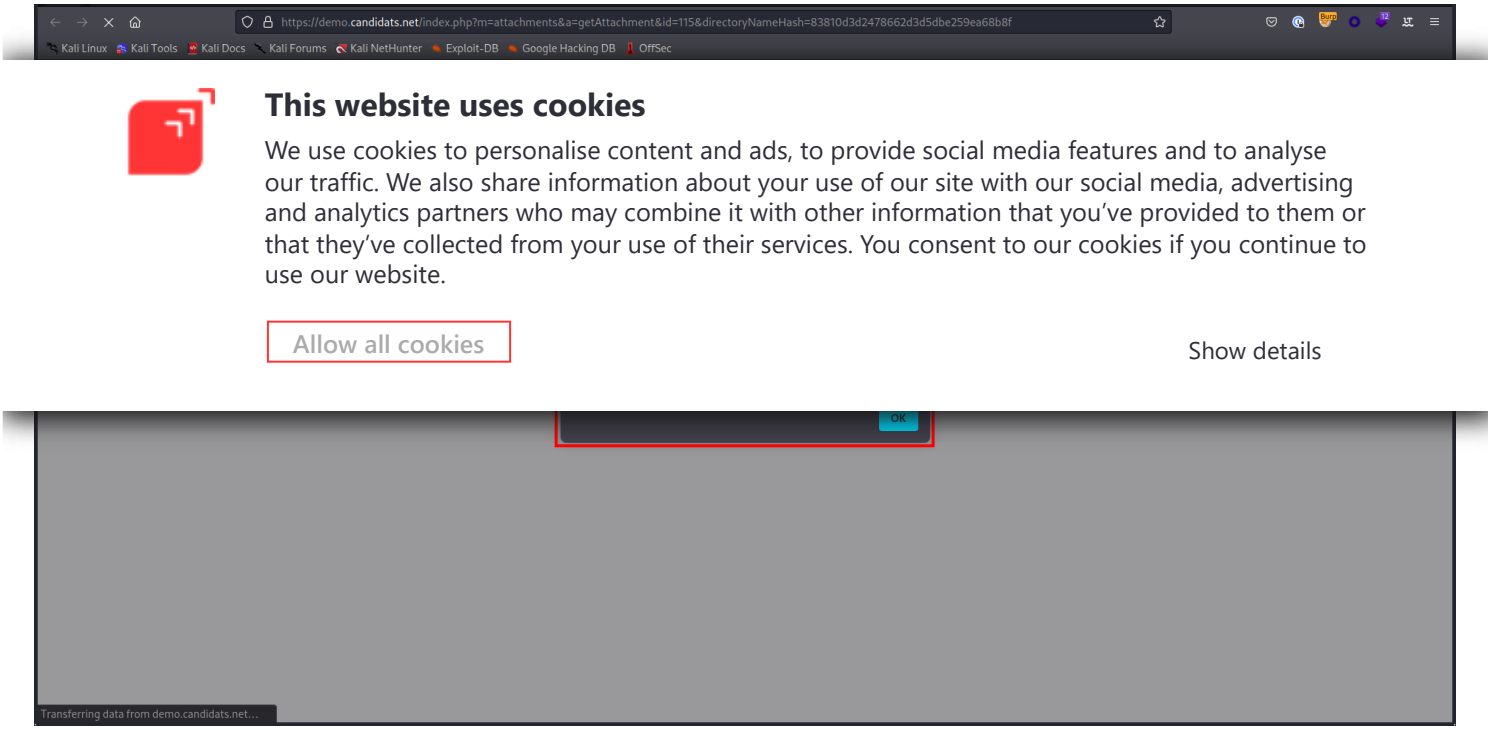
Vulnerability

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.





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.

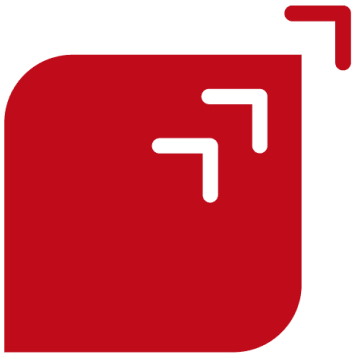
References

Vendor page https://candidats.net/

Vendor contacted.

2022-10-07
Vendor replied acknowledging the report.

2022-10-27
Public Disclosure.



Services

Secure Code Review

Red Teaming

Breach and Attack Simulation

Security Testing

Penetration Testing

Ethical Hacking

Vulnerability Management

Blog

Certifications

Partners