Local File Read in CandidATS 3.0.0 via XXE

Summary

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

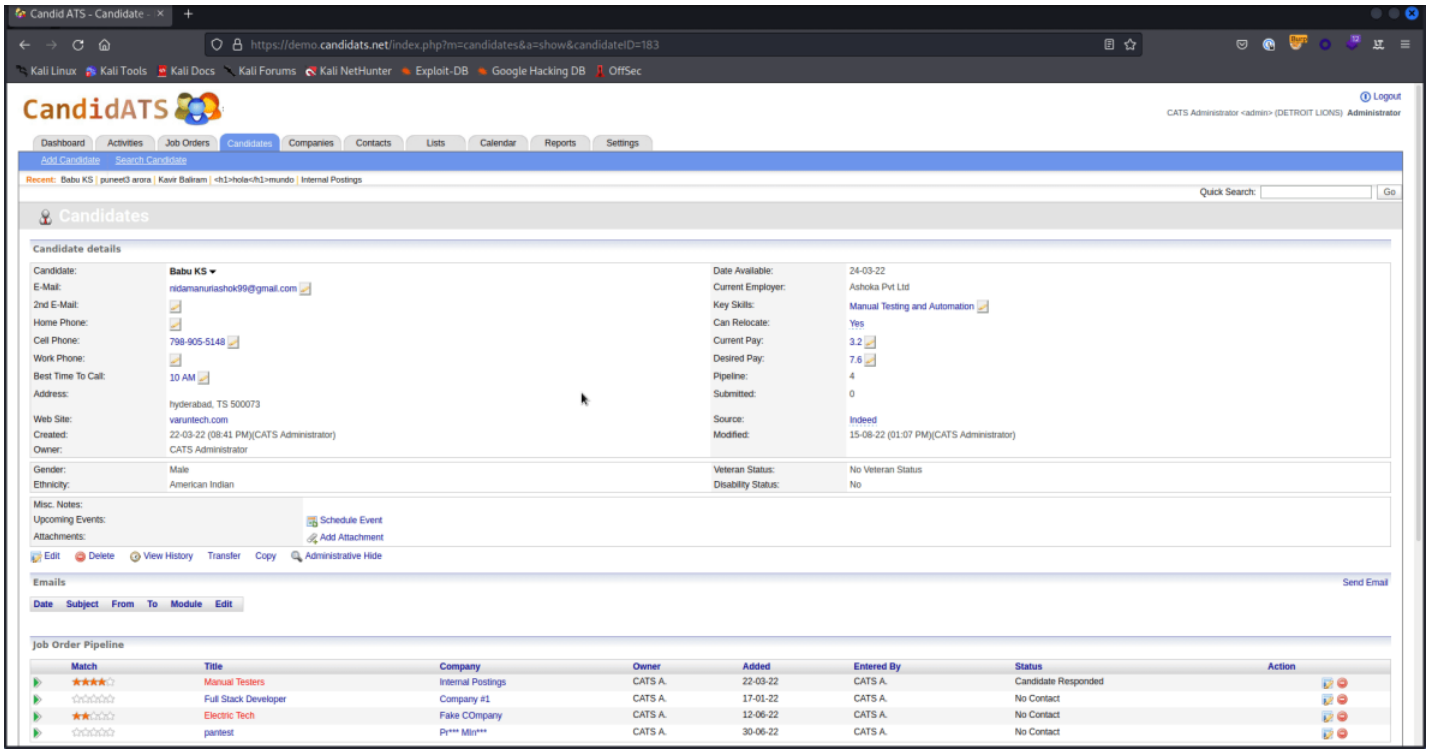
Vulnerability

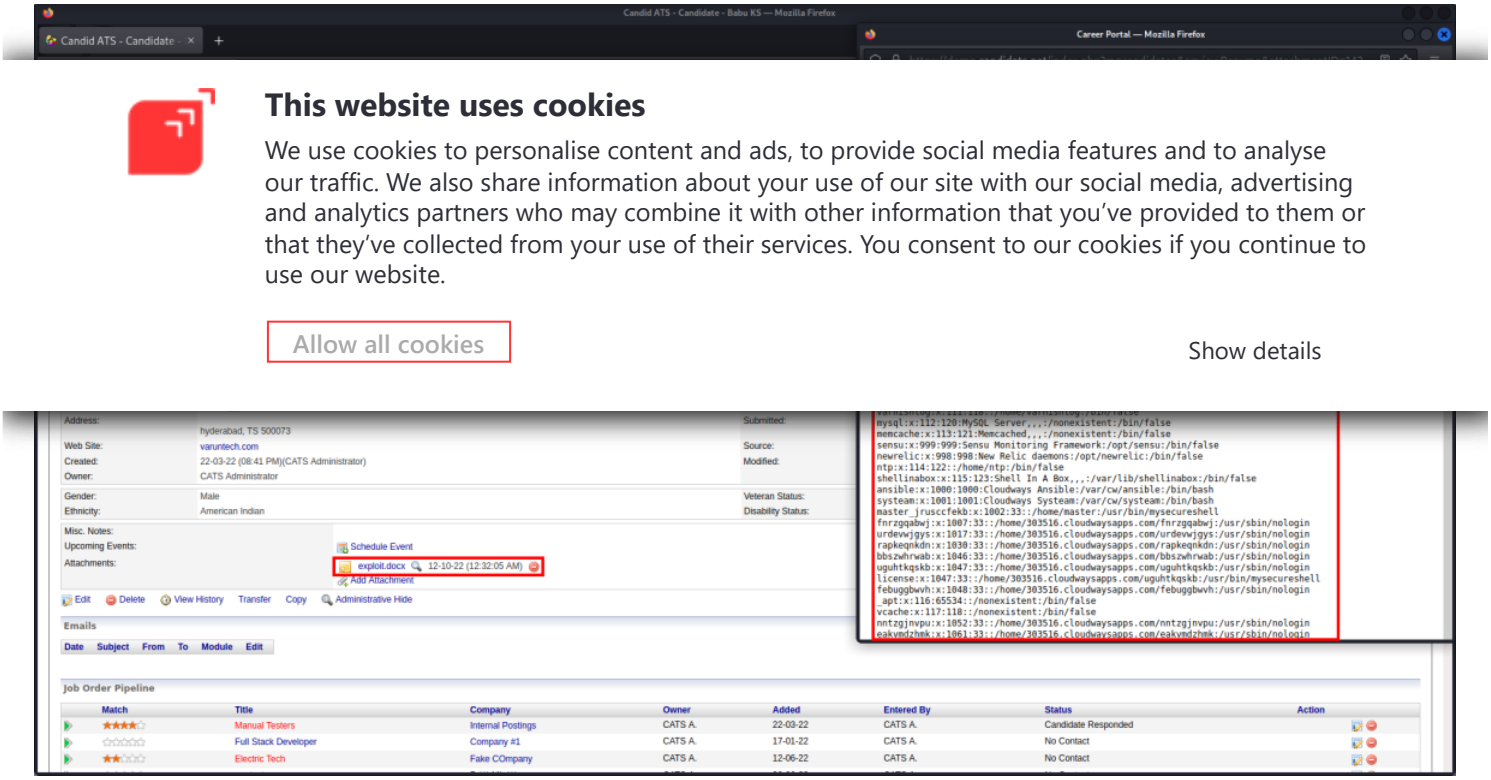
Kind	XML injection (XXE)
Rule	083. XML injection (XXE)
Remote	Yes
CVSSv3 Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
CVSSv3 Base Score	6.5
Exploit available	Yes
CVE ID(s)	CVE-2022-42745

The XXE present in CandidATS 3.0.0, allows an unauthenticated remote attacker to read arbitrary files from the server. To trigger this vulnerability, we will need to upload a malicious DOCX to the server.

Exploitation

In this attack we will be able to read arbitrary files from the server, through an XXE.





Our security policy

We have reserved the CVE-2022-42745 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

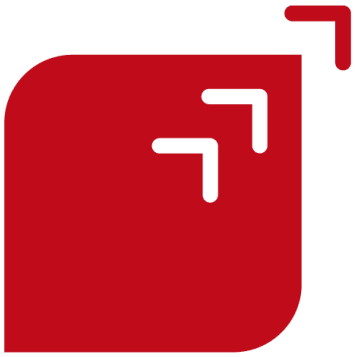
There is currently no patch available for this vulnerability.

Credits

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

References

- Vulnerability discovered.
- 2022-10-11
  Vendor contacted.
- 2022-10-11
  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