



Local File Read in CandidATS 3.0.0 via XXE

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	XML injection (XXE)
Rule	<u>083. XML injection (XXE)</u>
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)	<u>CVE-2022-42745</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

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.

CandidATS - Candidate - x +

https://demo.candidates.net/index.php?m=candidates&a=show&candidateID=183

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

CandidATS  [Logout](#)

CATS Administrator <admin> (DETROIT LIONS) Administrator

Dashboard | Activities | Job Orders | **Candidates** | Companies | Contacts | Lists | Calendar | Reports | Settings


Add Candidate Search Candidate


Recent: Babu KS | puneet3 anora | Kave Balram | xh1-hole-ch1-mundo | Internal Postings


Quick Search: Go


Candidates


Candidate details


Candidate: **Babu KS** 


E-Mail: nidamanurashok99@gmail.com 

2nd E-Mail: 

Home Phone: 

Cell Phone: 798-905-5148 

Work Phone: 

Best Time To Call: 10 AM 

Address: hyderabad, TS 500073


Web Site: varuntech.com

Created: 22-03-22 (08:41 PM) (CATS Administrator)


Owner: CATS Administrator


Date Available: 24-03-22

Current Employer: Ashoka Pvt Ltd

Key Skills: [Manual Testing and Automation](#) 

Can Relocate: Yes

Current Pay: 3.2 

Desired Pay: 7.6 

Pipeline: 4

Submitted: 0

Source: Indeed

Modified: 15-08-22 (01:07 PM) (CATS Administrator)


Gender: Male


Ethnicity: American Indian

Veteran Status: No Veteran Status

Disability Status: No

Misc. Notes:

Upcoming Events:  Schedule Event









Attachments:  Add Attachment

[Edit](#) [Delete](#) [View History](#) [Transfer](#) [Copy](#) [Administrative Hide](#)

Emails [Send Email](#)

[Date](#) [Subject](#) [From](#) [To](#) [Module](#) [Edit](#)

Job Order Pipeline

Match	Title	Company	Owner	Added	Entered By	Status	Action
★★★★★	Manual Testers	Internal Postings	CATS A.	22-03-22	CATS A.	Candidate Responded	 
☆☆☆☆☆	Full Stack Developer	Company #1	CATS A.	17-01-22	CATS A.	No Contact	 
★★★☆☆	Electric Tech	Fake Company	CATS A.	12-06-22	CATS A.	No Contact	 
☆☆☆☆☆	partest	Pr*** Min***	CATS A.	30-06-22	CATS A.	No Contact	 



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](#)

Address: hyderabad, TS 500073

Web Site: varuntech.com

Created: 22-03-22 (08:41 PM) (CATS Administrator)

Owner: CATS Administrator


Gender: Male



Ethnicity: American Indian

Veteran Status:

Disability Status:

Misc. Notes:

Upcoming Events:  Schedule Event







Attachments:  exploit.docx 12-10-22 (12:32:05 AM)  Add Attachment

[Edit](#) [Delete](#) [View History](#) [Transfer](#) [Copy](#) [Administrative Hide](#)

Emails [Send Email](#)

[Date](#) [Subject](#) [From](#) [To](#) [Module](#) [Edit](#)

Job Order Pipeline

Match	Title	Company	Owner	Added	Entered By	Status	Action
★★★★★	Manual Testers	Internal Postings	CATS A.	22-03-22	CATS A.	Candidate Responded	 
☆☆☆☆☆	Full Stack Developer	Company #1	CATS A.	17-01-22	CATS A.	No Contact	 
★★★☆☆	Electric Tech	Fake Company	CATS A.	12-06-22	CATS A.	No Contact	 

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



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 discovered.



2022-10-11

Vendor contacted.



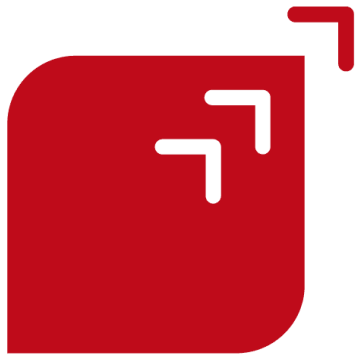
2022-10-11

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](#)