huntr

Uncontrolled Resource Consumption in causefx/organizr

0



Reported on May 11th 2022

Description

The Organizr application allows large characters to insert in the input field "Username" which can allow attackers to cause a Denial of Service (DoS) via a crafted HTTP request.

Proof of Concept

- 1. Sign up to the application, capture the request in burp suites, and send it to Repeater.
- 2.After the &username= parameter put the payload mentioned on this link:https://drive.google.com/file/d/1PBd3aXwKOL8uinLG7FJsn-8ldQceW4Zb/view?usp=sharing 3.Now press go and you will see the JWT token also get generated as the same size as the user input.

Video PoC

https://drive.google.com/file/d/1su5IYU3GwUBCMX6SP_Ur-u2uxXXPh6cT/view?usp=





Impact

This vulnerability can be abused by doing a DDoS attack for which genuine users will not able to access resources/applications.

References

Similar report

Vulnerability Type

CWE-190: Integer Overflow or Wraparound

Severity

Critical (9.9)

Registry

Packagist

Affected Version

2.1.1810

Visibility

Public

Status

Fixed

Found by



SAMPRIT DAS

@sampritdas8





Fixed by



causefx

a)causefx

unranked V

This report was seen 559 times.

We are processing your report and will contact the **causefx/organizr** team within 24 hours. 6 months ago

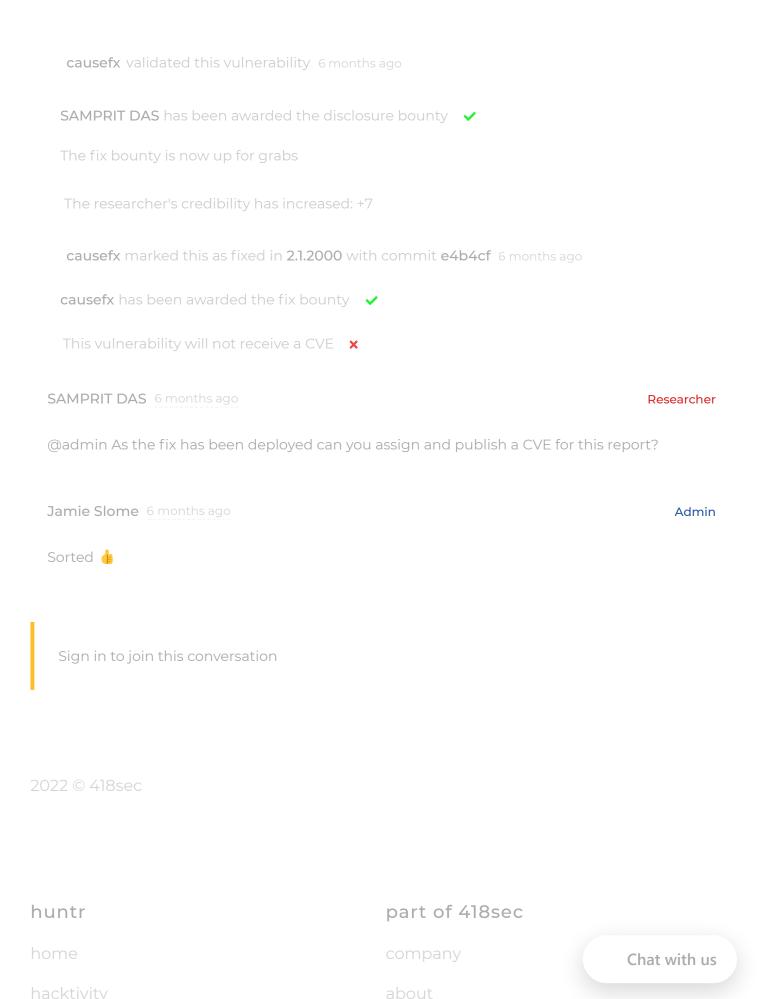
SAMPRIT DAS modified the report 6 months ago

SAMPRIT DAS modified the report 6 months ago

SAMPRIT DAS modified the report 6 months ago

Chat with us

SAMPRIT DAS modified the report 6 months ago



leaderboard team

FAQ

contact us

terms

privacy policy