huntr

Allowing long password leads to denial of service in causefx/organizr

0

✓ Valid Reported on May 11th 2022

Description

The Organizr application allows to sending a very long password (10000000 characters) it's possible to cause a denial of service attack on the server. This may lead to the website becoming unavailable or unresponsive. Usually, this problem is caused by a vulnerable password hashing implementation. When a long password is sent, the password hashing process will result in CPU and memory exhaustion.

Proof of Concept

1.Sign up to the application, capture the request in burp suites, and send it to Repeater.
2.Copy the payload from this link:-
https://drive.google.com/file/d/11AwLp8Ae1_eJqGb44W9QJDtPmVw-1RSQ/view?usp=sharing
and paste on password parameter and send go.
3.You will see that the application allows long passwords this can leads to Dos and can exploit as DDos

Video PoC

```
https://drive.google.com/file/d/1V_ZoXRJGkF7XSGdXJ4yPKRtQoxeTDyFe/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

- Drupal CVE-2014-9016

CVE
CVE-2022-1698
(Published)

Vulnerability Type
CWE-191: Integer Underflow (Wrap or Wraparound)

Severity
Critical (9.9)

Registry
Packagist

Affected Version
2.1.1810

Visibility
Public

Status
Fixed

Found by

SAMPRIT DAS
@sampritdas8
pro

Fixed by

causefx
@causefx
unranked

This report was seen 829 times.

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

causefx validated this vulnerability 6 months ago

SAMPRIT DAS has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

causefx marked this as fixed in **2.1.2000** with commit **e4b4cf** 6 months ago

causefx has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

SAMPRIT DAS 6 months ago Researcher

@admin As the fix has been deployed can you assign and publish a CVE for this report?

Jamie Slome 6 months ago Admin

Sorted 👍

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

part of 418sec

company

about

team

Chat with us

contact us

terms

privacy policy

Chat with us