

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

**Valid**

Reported on Mar 12th 2022

Proof of Concept

Go to add post <http://site.com/admin/post/create>

click on create new post

There will a option called `post title`

Fill the input field with huge characters, (more than 1 lakh)

Copy the below payload and put it in the input fields and click on continue.

You will see the application accepts large characters and if we will increase the characters then it can lead to Dos.

Download the payload from here:

<https://drive.google.com/file/d/1-e-1PMJx07zBhcZOGKipnq0j3C4ygDGA/view?usp=drivesdk>

Video & Image POC:

https://drive.google.com/drive/folders/1-L7kp5bmCuxBIEIxaUPu_lmKSOPpSdMU

Patch recemmondation:

The post title input should be limited to 500 characters or max 1000 characters.

References

- <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25062>

[Chat with us](#)

(Published)

Vulnerability Type

CWE-190: Integer Overflow or Wraparound

Severity

High (7.1)

Visibility

Public

Status

Fixed

Found by

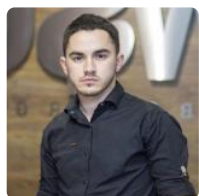


Akshay Ravi

@akshayravic09yc47

pro ▼

Fixed by



Bozhidar Slaveykov

@bobimicroweber

maintainer

This report was seen 572 times.

We are processing your report and will contact the **microweber** team within 24 hours.
8 months ago

Akshay Ravi modified the report 8 months ago

We have contacted a member of the **microweber** team and are waiting to hear back
8 months ago

Bozhidar Slaveykov validated this vulnerability 8 months ago

Akshay Ravi has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Bozhidar Slaveykov marked this as fixed in 1.2.12 with commit f7acbd 8 months ago

Chat with us

Bozhidar Slaveykov has been awarded the fix bounty 

This vulnerability will not receive a CVE 

Sign in to join this conversation

2022 © 418sec

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us