Able to create an account with long password leads to memory corruption / Integer Overflow in microweber/microweber

0

Valid Reported on Mar 17th 2022

I have found that there is a way to create an account with the length of more than 10k or 100k characters where it may leads to Integer overflow and the backend memory can't handle this issue

Steps to Reproduce:

Now we can create a simple account
While creating an account , In the password field we can able to input more than 10k or 100k characters in length
We can able to create 10k random string with the following Website Click Here
Generate random 10k/100k characters and Input them in password field
And the account will be created without any password length restriction

Impact:

By sending a very long password (1.000.000 characters) it's possible to cause a denial a 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. This vulnerability was detected by sending passwords with various lengths and comparing the measured response times.

CVE
CVE-2022-1036
(Published)

Vulnerability Type
CWE-190: Integer Overflow or Wraparound

Severity
Medium (5.3)

Visibility
Public

Status

Fixed

Found by

Nithissh12
@nithissh200
master

Fixed by

Bozhidar Slaveykov
@bobimicroweber
maintainer

This report was seen 815 times.

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

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

We have sent a follow up to the **microweber** team. We will try again in 7 days. 8 months ago

Bozhidar Slaveykov modified the report 8 months ago

Bozhidar Slaveykov validated this vulnerability 8 months ago

Nithissh12 has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Nithissh12 8 months ago — Researcher

Awesome :-)

Bozhidar Slaveykov marked this as fixed in **1.2.12** with commit **82be4f** 8 months ago

Bozhidar Slaveykov has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ×

Sign in to join this conversation