Weak Password Recovery Mechanism for Forgotten Password in microweber/microweber

1

Valid Reported on Feb 25th 2022

Description:

There is no rate limit sent unlimited email victim or any email address.

Proof of Concept:

There is no rate limit return-password , attacker to send unlimited email to victim or any email address.

Impact:

Attacker can sent unlimited email to any mail address .

Solution:

Add 'throttle' => 60, to auth.php config or $this->middleware('throttle:3,1') to the forgot password controller construct.

References

- https://github.com/laravel/laravel/blob/969ff64e02b5ba316ebfe58aba76ca9ceac34542/config/auth.php#L74-L96

CVE
CVE-2022-0777
(Published)

Vulnerability Type
CWE-640: Weak Password Recovery Mechanism for Forgotten Password

Severity
High (7.3)

Visibility
Public

Status
Fixed

Found by

HDVinnie
@hdvinnie
maintainer

Fixed by

Bozhidar Slaveykov
@bobimicroweber
maintainer

This report was seen 1,186 times.

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

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

Bozhidar Slaveykov validated this vulnerability 9 months ago

HDVinnie has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Bozhidar Slaveykov marked this as fixed in **1.3** with commit **a3944c** 9 months ago

Bozhidar Slaveykov has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation