huntr

Host Header injection in password Reset in livehelperchat/livehelperchat

0



Reported on Mar 11th 2022

Description

The password reset uses \$_SERVER['HTTP_HOST'] to generate the password without any checks or filtering. Allowing a malicious attacker to generate a fake password reset link to steal password reset tokens which may lead to account takeover

Impact

Account Takeover

Occurrences



normal forgotpassword.php L62

References

https://portswigger.net/web-security/host-header

CVE

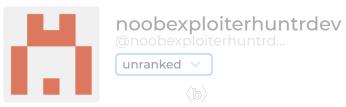
Vulnerability Type

Severity

Visibility

Chat with us

Found by



This report was seen 855 times.

We are processing your report and will contact the **livehelperchat** team within 24 hours.

9 months ago

Remigijus Kiminas validated this vulnerability 8 months ago

noobexploiterhuntrdev has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

noobexploiterhuntrdev 8 months ago

Researcher

Awesome, i did reproduced it in mine, here are some poc's just in case you need it

Click this link and You will be able to change a password </br>Restore password

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

We have sent a second fix follow up to the **livehelperchat** team. We will try again in 10 days. 8 months ago

We have sent a third and final fix follow up to the **livehelperchat** team. This report is now considered stale. 8 months ago

Remigijus 8 months ago

This was fixed. But seems some bug in hunter as I can't confirm a fix:D https://doc.livehelperchat.com/docs/security https://github.com/LiveHelperChat/livehelperchat/commit/ce96791cb4c7420274259ba7

Chat with us

Remigijus 8 months ago

@admin I'm a maintainer and I can't close the issue why?

Jamie Slome 8 months ago

Admin

@remdex - we have slightly adjusted our UI. You should be able to confirm the fix using the drop-down below.

You should see mark as fixed? Let me know if you are still having issues 👍

Remigijus Kiminas marked this as fixed in 3.97 with commit ce9679 8 months ago

The fix bounty has been dropped x

This vulnerability will not receive a CVE x

forgotpassword.php#L62 has been validated ✓

Sign in to join this conversation

2022 @ 418sec

huntr

homo

hacktivitv

leaderboard

part of 418sec

company

about

team

Chat with us

FAO

contact us

terms

privacy policy