Weak secrethash can be brute-forced in livehelperchat/livehelperchat

0

Valid Reported on Mar 29th 2022

Description

The `secrethash` , which the application relies for multiple security measures, can be brute-forced. The hash is quite small, with only 10 characters of only hexadecimal, making 16^10 possilibities (1.099.511.627.776). The SHA1 of the secret can be obtained via a captcha string and brute-forced offline with an GPU.

Proof of Concept

Get an Captcha String

Request

```
GET /index.php/captcha/captchastring/(timets)/1648529685 HTTP/1.1
Host: demo.livehelperchat.com
Cookie: lhc_vid=eb9bc0c044919538c5b1; PHPSESSID=qj7rpqcpcaipvphrals402aq7k
Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "macOS"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7
Connection: close
```

Chat with us

Response

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 29 Mar 2022 04:54:53 GMT
Content-Type: application/json
Connection: close
Vary: Accept-Encoding
X-Powered-By: PHP/7.4.27
Access-Control-Allow-Origin: *
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Origin, X-Requested-With, Content-Type, Accep
P3P: CP="IDC DSP COR ADM DEVi TAIi PSA PSD IVAi IVDi CONi HIS OUR IND CNT"
Expires: Sat, 26 Jul 1997 05:00:00 GMT
Last-Modified: Tue, 29 Mar 2022 12:54:53 GMT
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0
Pragma: no-cache
Content-Length: 53

{"result":"d04f714721f034d3abaccbb0ee755e31dac8fc2b"}
```

The result is equal to :

```
$hash = sha1(erLhcoreClassIPDetect::getIP().$Params['user_parameters']['tim
```

All the `sha1()` function's inputs are known to the attacker, but the `secrethash` . With this SHA1 it's possible to brute force the `secrethash` using `hashcat` for example. I didn't start a PoC to prove it's feasible to not waste computional power, but I have a 2060 RTX and did some calculations and it could crack within a week or so.

Impact

An attacker could crack the `secrethash` and use it to bypass security measu

Chat with us

Occurrences

install.php L167 captchastring.php L11

CVE
CVE-2022-1235
(Published)

Vulnerability Type
CWE-916: Use of Password Hash With Insufficient Computational Effort

Severity
High (7.5)

Visibility
Public

Status
Fixed

Found by

Caio Lüders
@caioluders
legend

This report was seen 743 times.

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

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

Remigijus 8 months ago Maintainer

Sorry, but I don't see any value in your report, if it will take a week, the catch will be expired at that time as it's valid only for 30m :)

Chat with us

Remigijus 8 months ago Maintainer

And how exactly you can abuse even if you quest a hash?

Caio Lüders 8 months ago Researcher

Hello Remigijus,

The cracking isn't of the Captcha itself, but discovering the value of `secrethash`. As the `secrethash` doesn't expire an attacker can bypass a series of validations, `secrethash` is used on 27 points of the software. To the best of my knowledge, `secrethash` is used to validate the legitimacy of readchat, paidchat and as a salt on the passwords, among other things.

Also, the week was just of an example on my hardware, on a better hardware this could probably done in a day or two.

Remigijus 8 months ago Maintainer

ok, now I understood your point. Just need the better generator for the secret hash value itself.

Remigijus Kiminas validated this vulnerability 8 months ago

Caio Lüders has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Remigijus Kiminas marked this as fixed in 3.96 with commit 6538d6 8 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

captchastring.php#L11 has been validated ✓

install.php#L167 has been validated ✓

Remigijus 8 months ago Maintainer

Changed to https://github.com/LiveHelperChat/livehelperchat/blob/master/lhc_web/lib/cc
p#L1379 and length with be 80 characters.

Chat with us

Jamie Slome 8 months ago Admin

@remdex - the researcher has requested a CVE for this report. Are you happy for us to assign and publish one?

Remigijus 8 months ago Maintainer

Yes you can.

Jamie Slome 8 months ago Admin

Sorted ♥

Sign in to join this conversation

2022 © 418sec

Chat with us