Sensitive Cookie Without 'HttpOnly' Flag in pi-hole/adminlte

0

✓ Valid Reported on Sep 1st 2021

✍️ Description

Please enter a description of the vulnerability. The cookie `persistentlogin` is set without httponly flag

🕵️ Proof of Concept

Enable remember me during Login

```
POST /admin/index.php?login HTTP/1.1
Host: 192.168.159.138
Content-Length: 30
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.159.138
Content-Type: application/x-www-form-urlencoded
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
Referer: http://192.168.159.138/admin/index.php?login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=qfv8v7h8r6jrfsark4in9ia2ue
Connection: close

pw=***&persistentlogin=on
```

```
HTTP/1.1 302 Found
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=***; path=/; HttpOnly
Set-Cookie: persistentlogin=***; expires=Wed, 08-Sep-2021 18:36:11 GMT; Max
Location: index.php
Content-type: text/html; charset=UTF-8
X-Pi-hole: The Pi-hole Web interface is working!
X-Frame-Options: DENY
Content-Length: 0
Connection: close
Date: Wed, 01 Sep 2021 18:36:11 GMT
Server: lighttpd/1.4.53
```

💥 Impact

Steal cookies with XSS.

Occurrences

🐘 password.php L82

References

- HttpOnly

CVE
CVE-2021-3706
(Published)

Vulnerability Type
CWE-1004: Sensitive Cookie Without 'HttpOnly' Flag

Severity
High (7.4)

Chat with us

Affected Version
*

Visibility
Public

Status
Fixed

Found by

wtwver
@wtwver
unranked

Fixed by

wtwver
@wtwver
unranked

This report was seen 586 times.

We have contacted a member of the **pi-hole/adminlte** team and are waiting to hear back
a year ago

wtwver submitted a patch a year ago

Adam Warner validated this vulnerability a year ago

wtwver has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Adam Warner a year ago Maintainer

@wtwver, the patch you've submitted isn't quite right - the use of named parameters only works in PHP >=8 (https://stackoverflow.com/a/36885)

As we have to support lower versions, it needs to go the way of:

```
setcookie('persistentlogin', $pwhash, time()+60*60*24*7, null, null, null, true );
```

There is also an additional place that it needs to be changed in.

Interestingly, on line 13 we already call `ini_set('session.cookie_httponly',1)` so this is clearly a bridge we've tried to cross before - but I guess calling `setcookie` with `httponly=false` overrides that.

Adam Warner a year ago Maintainer

That said, I've no interest in the bounty so I'll award it to you once we merge it into master

wtwver a year ago Researcher

Hi thanks for the reply and the bounty

It seems that the code on line 13 only apply to the phpsessid cookie

Btw, do u think will there be any cve for this and other xss?

Thanks

Adam Warner a year ago Maintainer

I really don't know how this huntr.dev system works - it's all new to me. I think they organise it from here. Usually I would do it through the Security Advisories feature on github, but I don't want to double up the effort :S

@admin maybe you could provide some pointers here? (is that how you summon the admin??)

Adam Warner marked this as fixed with commit cf8602 a year ago

wtwver has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Jamie Slome a year ago Admin

@promofaux - we can assign a CVE for this, and would be happy to do it on your behalf.

Any validated vulnerability via our platform can be awarded a CVE. Currently, our CVE assignment process is in beta, and so we only allow a select few through the system automatically, but I am more than happy to arrange this for you myself.

Would you both be happy for me to go ahead and issue a CVE?

wtwver a year ago Researcher

Sure

Jamie Slome a year ago Admin

CVE published here!

It should appear on the National Vulnerability Database shortly.

Great work all.

Adam Warner a year ago Maintainer

https://github.com/pi-hole/AdminLTE/security/advisories/GHSA-9hfp-j66v-6q3j

Sign in to join this conversation