Stored DOM XSS in Pi-hole Admin Web Interface v5.4

Moderate **PromoFaux** published **GHSA-cwwf-93p7-73j9** on Apr 14, 2021

Package

Pi-hole Admin Interface

Affected versions	Patched versions
<=5.4	5.5

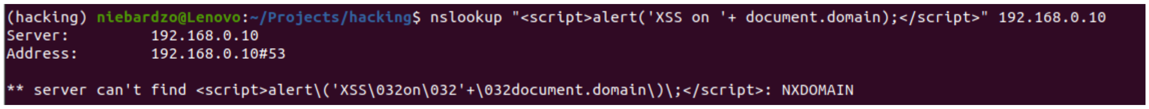
Description

The Stored XSS exists in the Pi-hole Admin portal, which can be exploited by the malicious actor with the network access to DNS server.

Versions: Pi-hole v5.2.4 Web Interface v5.4 FTL v5.7
CVSS vector: AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:H
CVSS3.0 base score: 7.6

Steps to replicate:

1. Few times resolving the XSS (as domain) with the Pi-Hole DNS server e.g.
   $ nslookup "<script>alert('XSS on '+ document.domain);</script>" 192.168.0.10



```
(hacking) niebardzo@Lenovo:~/Projects/hacking$ nslookup "<script>alert('XSS on '+ document.domain);</script>" 192.168.0.10
Server:         192.168.0.10
Address:        192.168.0.10#53

** server can't find <script>alert\('XSS\032on\032'+\032document.domain\)\;</script>: NXDOMAIN
```

192.168.0.10 is the local IP of my Pi.

2. Simulate the victim by authenticating to Pi-hole Web Interface, then go to the Long-term data -> Query log tab.
3. Select today's data and find the row in the table with XSS payload.
4. Click on the Blacklist button and see the alert box.

Rationale behind the CVSS vector:

The exploitation requires network access to the Pi-hole DNS Server and the victim's interaction. As the admin panel allows for the switching off the PiHole, the impact on availability is high. Regarding integrity and confidentiality, the threat actor can do the same actions as admin and access the same data as admin, the impact is low as the UI options pretty limit the administrator in its capabilities.

Severity

Moderate

CVE ID

CVE-2021-29448

Weaknesses

No CWEs

Credits

niebardzo