Authorization bypass: CLI API sessions can import Teleporter archives and modify configuration

Moderate **PromoFaux** published **GHSA-r7g8-3fj7-m5qq** 4 days ago

Package

pi-hole/ftl

Affected versions

>= 6.0, <= 6.5

Patched versions

6.6

Description

Summary

Pi-hole FTL supports a CLI password feature (`webserver.api.cli_pw`) that creates “CLI” API sessions intended to be read-only for configuration changes. While `/api/config` correctly blocks CLI sessions from mutating configuration, `/api/teleporter` allowed Teleporter imports for CLI sessions, enabling a CLI-scoped session to overwrite configuration via a Teleporter archive (authorization bypass).

Details

- CLI sessions are flagged via `session->cli` (set when authenticating with the CLI password).
- `/api/config` blocks CLI sessions by returning HTTP 403 when `api->session->cli` is true.
- `/api/teleporter` did not perform the same check before processing an uploaded Teleporter archive (e.g., ZIP imports can overwrite `etc/pihole/pihole.toml`; legacy Teleporter TAR.GZ imports can restore additional config files).
- Expected behavior: Teleporter import should be restricted to fully privileged sessions, not CLI sessions.

PoC (local lab)

Prereqs: API password set; CLI password feature enabled (`webserver.api.cli_pw=true` / `FTLCONF_webserver_api_cli_pw=true`).

1. Obtain the CLI password (in a lab it is stored at `/etc/pihole/cli_pw`) and authenticate to get a `sid`:

- `POST /api/auth` with the CLI password

2. Confirm CLI sessions are blocked from config changes (expected behavior):

- Try any config-changing request to `/api/config` and observe HTTP 403 `forbidden`

3. Demonstrate the bypass via Teleporter import:

- Download a Teleporter archive: `GET /api/teleporter`
- Import it back using the same CLI session: `POST /api/teleporter` with the archive as multipart form field `file`
- Observe the import succeeds (and triggers a restart) despite being a CLI session

Impact

An attacker who obtains CLI-scoped API credentials can modify Pi-hole configuration through the Teleporter import endpoint, bypassing intended authorization restrictions for CLI sessions.
This can be used to change settings (e.g., disable blocking, alter upstream DNS, change DHCP settings), impacting integrity/availability.

Suggested fix

Add the same CLI-session restriction used by `/api/config` to `/api/teleporter` (reject when `api->session->cli` is true).

Severity

Moderate 6.1 / 10

CVSS v3 base metrics

Attack vector	Local
Attack complexity	Low
Privileges required	Low
User interaction	None
Scope	Unchanged
Confidentiality	None
Integrity	High

Availability	Low

Learn more about base metrics

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:L

CVE ID

CVE-2026-35491

Weaknesses

▶ CWE-863

Credits

mzalzahrani Reporter