0-DAY NO CVE HIGH PUBLIC

OPNsense 26.7.6 factory LOG_AUTH plants sshlockout

OPNsense core 26.7.6 unauth WebGUI login still drives lockout_handler from a factory LOG_AUTH line with no socket IP. Last-token pick, the GHSA-2v2x hardening, plants an attacker-chosen address into sshlockout. Labbed.

NAME OPNsense 26.7.6 factory LOG_AUTH plants sshlockout	TYPE 0-day analysis
CVE n/a	CVE RISK high
DISCLOSURE STATUS public	VENDOR OPNsense (Deciso B.V.)
AFFECTED OPNsense core 26.7.6 (a842fe48) AuthenticationFactory syslog plus lockout_handler last-IP. Default lockout on, LAN GUI. Unauth login POST.	PUBLISHED 13 Oct 2026
UPDATED 13 Oct 2026	TAGS 0-day, opnsense, lockout, privilege-leftover, cwe-117, cwe-863

TL;DR

Lab files and proof-of-concept **here**.

01 Last-IP saved authgui. It did not save the factory line.

I am @abraxas_null. The proof of concept is on GitHub: **abraxas/opnsense-lockout-factory-ip** (loopback client). The lab stack is `lab/`. Authorized lab only. It talks to loopback.

This is **OPNsense core 26.7.6** (`a842fe48c21288d11a422cb944678e8eb308becf`). No CVE yet. CWE-117 / CWE-863. 7.5 High (`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H`). Remote unauthenticated privilege leftover. Default: lockout on, LAN GUI.

GHSA-2v2x closed CRLF split. syslog-ng rewrites CR/LF to space. IP pick moved to the **last** token so `authgui.inc` 's trailing `from REMOTE_ADDR` wins. That is the right hardening for the authgui template. `AuthenticationFactory::authenticate()` still `syslog(LOG_WARNING, "user %s could not authenticate for %s. [using %s + %s]", $username, ...)` with **no** socket IP. A username that matches a lockout False phrase plus an IPv4 token is the last (only) address on that line. After default 5 spaced attempts: `pfctl -t sshlockout -T add` and `pfctl -k` .

This is not CRLF. One PHP syslog record stays one handler line. Last-IP was the wrong hardening for the factory template.

02 Why OPNsense

Same pin as the rest of this 26.7.6 pass. I wanted leftovers of public GHSAs, not a re-file of the named walk. Lockout is default-on. Unauth login POST is the front door. If the factory line still plants a table, that is High availability of SSH and GUI from a chosen host. Not a login skip. Not RCE.

03 Pinning 26.7.6

Tag `26.7.6` peel `a842fe48c21288d11a422cb944678e8eb308becf`. Not master. Not 27.1.a. Not EOL 26.1. 26.7.6 also changed `pfctl -k str(ip)` (Omar Habra). That TypeError is already on this pin. I did not keep it.

04 The skip list is half the hunt

I did not re-file:

- GHSA-2v2x itself. CRLF extra `readline()`. First IPv4 wins. Closed. IP pick is last token. authgui still ends with `REMOTE_ADDR`.
- CVE-2026-44195 / GHSA-h3vx success-keyword counter reset. Failure rules now precede `Accepted` / `Successful login`. Username `Accepted` on the **authgui** line matches `Web GUI authentication error` first.
- GHSA-x3q7 empty-password Save. 26.7.5.
- GHSA-jjm2 audit log injection via login username. Write-side LF. Integrity of the audit file is Medium. The High pf-table walk is this leftover, not that GHSA.
- CVE-2026-34578 LDAP filter injection. `ldap_escape`. Empty password returns false before bind.
- Empty-password login. `authgui.inc` requires a non-empty password.
- 26.7.6 Omar Habra `pfctl -k str(ip)` TypeError.

Twenty-eight hunts. This is G2. Default WebGUI. Unauth.

05 How the factory line plants an IP

Unauth POST `/index.php` with `login=1`, non-empty `usernamefld` / `passwordfld`. CSRF cookie plus token from GET `/`. `authgui.inc` calls `AuthenticationFactory::authenticate("WebGui", username, password)`. On failure the factory always syslog's the raw username after `openlog(..., LOG_AUTH)`. That string has no `REMOTE_ADDR`.

syslog-ng `facility(auth)` feeds `lockout_handler`. Handler walks tokens, keeps the last `ipaddress.ip_address`. First matching `all_rules` key wins. `.*Web GUI authentication error.*` is False (block). The factory message is not an authgui line, but a username that contains that phrase still matches `re.match` from the start because of the leading `.*`.

authgui's own error log still ends `from {REMOTE_ADDR}`, so last-IP on **that** line is the attacker. The factory line's last IP is whatever token sat in the username. Counts are per IP. Default `--attempts 5`. Timestamps more than 2s apart. Six spaced POSTs add the planted address.

pf then blocks TCP from that table to `(self)` ports 22 and WebGUI and kills states sourced from that host.

06 Wrong turns, in order

I first tried to re-file GHSA-2v2x. CRLF is gone. Then I assumed last-IP closed every plant. It closed the authgui plant of a foreign IP. It opened the factory plant of a foreign IP. Then I sent a username that was only the IPv4. No False phrase. No table add. Then I looked at empty-password login. Closed. Then I looked at 44195 success-keyword reset on the authgui line. Failure rules first. Then Omar Habra's `str(ip)` TypeError. Already on this pin.

Anti-lockout pass on the primary interface may still let a LAN operator reconnect after state kill. I did not treat that as a full close. WAN or non-primary-interface

admins stay behind the table. `pfctl -k` still drops the live session.

07 The lab

Pinned `lockout_handler` copied unchanged. PATH stub `pfctl`. syslog-ng and WebGUI POST stubbed. Loopback identity `127.0.0.1:18800`. Compose project `opnsense-lockout-factory-ip`. Image tag `opnsense-lockout-factory-ip:26.7.6`.

CONTROL: username is only `203.0.113.77`. No table add. `negative-ip-only=no`. TRIGGER: username `Web GUI authentication error 203.0.113.77`. Six spaced factory lines. Table add plus kill argv. AUTHGUI control: trailing `from 198.51.100.10` stays last-IP.

Last run:

PLAIN TEXT Copy

```
SUCCESS opnsense-lockout-factory-ip planted=203.0.113.77 table=sshlockout negativ
```

Live pf drop of TCP 22/GUI and live session kill stay inferred. Gadget, not a full OPNsense VM.

08 What an attacker can do

METHOD

Unauth factory `LOG_AUTH` username with a lockout False phrase plus an IPv4 token (6 spaced

METHOD
same plant, live pf
same username with only the IPv4 (no False phrase)
authgui line with trailing `from REMOTE_ADDR`
Failed-login body

Requires: Unauth WebGUI login POST. CSRF cookie + token from GET `/`. Lockout on (`system.no_sshlockout` unset). Default install.

09 Adjacent surface that stays closed

Unauth session / root / `config.xml` write. authgui line planting a foreign IP (last token is `REMOTE_ADDR`). CRLF extra `readline()`. Empty-password login. CVE-2026-44195 success-keyword reset on the authgui line. 26.7.6 Omar Habra `pfctl -k str(ip)` TypeError. Does not block the planted IP as a DNS/gateway destination (rules are `from <sshlockout> to (self)` ports 22/GUI only). Does not mint a session.

10 The fix

Append the socket IP to the factory `syslog(LOG_AUTH)` template, same trailing `from REMOTE_ADDR` as `authgui.inc`. Or ignore lockout IPs that did not come from the handler's own peer. Do not treat last-token as a substitute for "the client address."

Replay:

PLAIN TEXT Copy

```
cd lab
./run.sh
```

Loopback `127.0.0.1:18800`. Witness `OPNSENSE-LOCKOUT-FACTORY-IP-WITNESS`.

11 References

- Pack: github.com/abraxas/opnsense-lockout-factory-ip
- Product: github.com/opnsense/core `a842fe48c21288d11a422cb944678e8eb308becf`
- `AuthenticationFactory.php`
- `lockout_handler`
- Named walk (not this leftover): GHSA-2v2x
- CWE-117 / CWE-863

Abraxas Labs https://abraxaslabs.tech https://github.com/abraxas https://x.com/abraxas_null (`@abraxas_null`) abraxas.null@proton.me

Abraxas Labs

Independent security research by abraxas.

Analysis of 0-days, n-days, malware, and the

leftovers that still matter.

GitHub **@abraxas_null** **abraxas.null@proton.me** **abraxaslabs.tech**

Independent research. Private analysis by arrangement. No ads. abraxas.null@proton.me · For defensive awareness and authorized testing only.

© 2026 Abraxas Labs