0-DAY NO CVE HIGH PUBLIC

OPNsense 26.7.6 WLAN WPA identity line injection

OPNsense core 26.7.6 wireless SSID got AllowNewlines=N. WPA identity, passphrase, and RADIUS secret stayed bare TextField and dump into wpa_supplicant/hostapd conf. Delegated page-interfaces-wireless-edit. Labbed.

NAME **OPNsense 26.7.6 WLAN WPA identity line injection**	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) Wlan.xml identity/passphrase plus interfaces_wlan_configure. Privilege page-interfaces-wireless-edit. SSID already rejects CR/LF.**	PUBLISHED **13 Oct 2026**
UPDATED **13 Oct 2026**	TAGS **0-day, opnsense, wlan, line-injection, cwe-93**

TL;DR

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

01 SSID learned. Identity did not.

I am @abraxas_null. The proof of concept is on GitHub: **abraxas/opnsense-wlan-wpa-line** (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-93. 8.1 High (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N`). Remote authenticated config line injection. Privilege `page-interfaces-wireless-edit`. Not `page-all`.

GHSA-fq94 converted a pile of GUI text that landed in generated service conf. Wireless SSID on the same model was given `AllowNewlines=N`. `wpa.identity`, `wpa.passphrase`, `auth_server_shared_secret`, and `auth_server_shared_secret2` stayed plain `TextField`. `TextField` defaults `internalAllowNewlines = true`. `interfaces.inc` interpolates `identity="{identity}"` and `password="{passphrase}"` into `/var/etc/wpa_supplicant_*.conf`. Hostap writes unquoted `wpa_passphrase=` and `auth_server_shared_secret=` into `/var/etc/hostapd_*.conf`. Newline or quote break adds extra directives. Those daemons run as root.

02 Why OPNsense

Same 26.7.6 pin. I hunted leftovers of fq94, not a re-file of the named fields. A delegated wireless editor is allowed to set an identity. That editor was not meant to mint extra `network={}` blocks, `ctrl_interface`, or `ap_scan`. Full admin already has root by design. The leftover is the extra line.

03 Pinning 26.7.6

Tag `26.7.6` peel `a842fe48c21288d11a422cb944678e8eb308becf`. Not master. Not 27.1.a. Not EOL 26.1.

04 The skip list is half the hunt

I did not re-file:

- GHSA-fq94 itself. Named sinks converted. Hunt is leftover of that fix.
- SSID newline. Already `AllowNewlines=N`.
- GHSA-6vv6 cert/CA description in wireless EAP. Cert payload path, not these WPA text fields.
- CVE-2025-50989 bridge span cmdi. Now `configdRun` with no request token.
- WEP keys. `escapeshellarg` into `ifconfig`.
- CVE-2026-49131 / 49132 stored XSS descriptions. HTML only.

Twenty-eight hunts. This is G4. NTP GPS fudge is G3, same class, different ACL.

05 How identity becomes a second wpa_supplicant line

MVC save is `WirelessSettingsController` under ACL `page-interfaces-wireless-edit` (`ui/interfaces/wireless`, `api/interfaces/wireless_settings/*`). POST `/api/interfaces/wireless_settings/*`. Wireless clone apply already restarts hostapd / wpa_supplicant as root.

`interfaces.inc` then interpolates those strings with no further strip:

- BSS / wpa_supplicant: `password="…"`, `identity="…"`, `psk="…"`, then a heredoc written to `/var/etc/wpa_supplicant_{device}.conf`.
- Hostap: unquoted `wpa_passphrase={…}` and unquoted `auth_server_shared_secret={…}` written to `/var/etc/hostapd_{device}.conf`.

A newline or a quote break ends the intended assignment and starts a new directive. Inferred extras include `ctrl_interface` / `ctrl_interface_group`, `pkcs11_module_path` / `opensc_engine_path`, extra `network={…}` blocks, `eap_user_file` / `wpa_psk_file`.

A browser `<input type="text">` will not keep CR/LF. A direct POST from that session will.

06 Wrong turns, in order

I first assumed SSID `AllowNewlines=N` meant the whole Wlan.xml block had been converted. Identity is a sibling field with no such flag. Then I looked at WEP. Quoted through `escapeshellarg`. Then I looked at 50989 bridge cmdi. Closed. Then I looked at cert description in EAP. GHSA-6vv6. Skip. Then I wondered whether `page-all` was the intended bar. A wireless editor is supposed to set a passphrase. Extra hostapd directives are not that page.

I almost stopped at "wpa_supplicant not started." The leftover is the extra line in the conf the daemon will load. Honor of extra `network` / `ssid` / `ap_scan` stays inferred. The gadget proves the write.

07 The lab

PHP 8.3 gadget of pinned `interfaces_wlan_configure`. Interpolation lines stay byte-identical in `pin/interfaces.inc`. No wpa_supplicant. Loopback HTTP on `127.0.0.1:18840`. Compose project `opnsense-wlan-wpa-line`.

CONTROL: identity `user`, SSID `lab-ssid`. One identity line, one ssid line, no witness. TRIGGER: identity `user` plus CR/LF plus `# OPNSENSE-WLAN-WPA-LINE-WITNESS`. Extra directive after identity. SSID stayed one line.

Last run:

PLAIN TEXT Copy

```
SUCCESS opnsense-wlan-wpa-line identity-newline=yes extra-directive=yes ssid-cont
```

hostapd and live daemon apply stay inferred. Gadget, not a full OPNsense VM.

08 What an attacker can do

METHOD	SINK
identity CR/LF	pin `interfaces_wlan_configure` extra directive in `wpa_supplicant` conf
honor of extra `network` / `ssid` / `ap_scan` / `ctrl_interface`	wpa_supplicant / hostapd as root

METHOD	SINK
SSID CR/LF	`AllowNewlines=N`
passphrase / RADIUS secret CR/LF	`hostapd_*.conf` / `wpa_supplicant`
invalid extra directive	wireless daemons
this path	none

Requires: `page-interfaces-wireless-edit`. POST `/api/interfaces/wireless_settings/*`. Not `page-all`. CSRF token.

09 Adjacent surface that stays closed

SSID newline (constrained). Unauth. `page-all` wireless admin (intended radio config; leftover is extra directives a delegated editor was not meant to mint). CVE-2025-50989 bridge span cmdi. WEP keys `escapeshellarg`'d into `ifconfig`.

10 The fix

Set `AllowNewlines=N` on `identity`, `passphrase`, and RADIUS secrets, same as SSID. Strip CR/LF and quotes inside `interfaces_wlan_configure` so every caller is covered. Extra hostapd / wpa_supplicant directives belong behind `page-all`.

Replay:

PLAIN TEXT Copy

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

Loopback `127.0.0.1:18840`. Witness `OPNSENSE-WLAN-WPA-LINE-WITNESS`.

11 References

- Pack: github.com/abraxas/opnsense-wlan-wpa-line
- Product: github.com/opnsense/core `a842fe48c21288d11a422cb944678e8eb308becf`
- `Wlan.xml`
- `interfaces.inc` `interfaces_wlan_configure`
- Named fields (not this leftover): GHSA-fq94; SSID `AllowNewlines=N`

- CWE-93

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**

Home Research Open Source Reading Room About GitHub @abraxas_null Console

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

© 2026 Abraxas Labs