0-DAY NO CVE HIGH PUBLIC

OPNsense 26.7.6 NTP GPS fudge line injection

OPNsense core 26.7.6 GPS/PPS fudge1/fudge2/refid still concatenate into ntpd.conf after GHSA-fq94 stripped timeserver hosts. Delegated page-services-ntp-gps. Labbed.

NAME OPNsense 26.7.6 NTP GPS fudge 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) ntpd.inc GPS/PPS fudge. Privilege page-services-ntp-gps and/or page-services-ntp-pps. Timeserver host CR/LF already stripped.	PUBLISHED 13 Oct 2026
UPDATED 13 Oct 2026	TAGS 0-day, opnsense, ntp, line-injection, cwe-93, cwe-74

TL;DR

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

01 Timeservers got the strip. GPS fudge did not.

I am @abraxas_null. The proof of concept is on GitHub: **abraxas/opnsense-ntp-gps-fudge** (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 / CWE-74. 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-services-ntp-gps` and/or `page-services-ntp-pps`. Not `page-all`.

GHSA-fq94 named NTP timeserver input into `/var/etc/ntpd.conf`. `ntpd_configure_do` now strips CR/LF on each timeserver token. GPS/PPS `fudge1` / `fudge2` / `refid` sit on the same `fudge` line and never got that strip. The general NTP page already treats extra ntpd.conf text as escalation (`userIsAdmin` on `custom_options`). GPS/PPS ACLs are separate pages. Save runs `configd_run('service restart ntpd')`. ntpd starts as root with no `-u`.

CVE-2026-53581 was a serial path overwrite. That path is allowlisted (`^cua[a-z0-9.,{}]+$` plus a char device). `../` no longer leaves `/dev/`. This leftover is the text next to that path.

02 Why OPNsense

Same 26.7.6 pin. I hunted leftovers of public GHSAs. fq94 converted a pile of GUI text to `StrictTextField` or a sink-side strip. Two delegated surfaces were not converted: NTP GPS/PPS fudge, and wireless WPA identity. This is the NTP one.

03 Pinning 26.7.6

Tag `26.7.6` peel `a842fe48c21288d11a422cb944678e8eb308becf`. Not master. Not 27.1.a. Not EOL 26.1. Plugins and the FreeBSD tree are out.

04 The skip list is half the hunt

I did not re-file:

- CVE-2026-53581 / GHSA-872g GPS/PPS serial path traversal. `preg_match('/^cua[a-z0-9.,{}]+$/i', $port)` plus a char node. DROP as originally filed.
- GHSA-h793 stored XSS NTP GPS initcmd. Decode then `legacy_html_escape_form_data`. No chain to this High.
- GHSA-fq94 timeserver host CR/LF. Stripped at `ntpd.inc:327-329`.
- `custom_options` on `services_ntpd.php`. Admin-gated for this exact reason.
- Leap-seconds upload to hardcoded `/var/db/leap-seconds`.
- Documented xmlrpc HA with shared root password.

Twenty-eight hunts. This is G3.

05 How fudge becomes a second ntpd.conf line

`services_ntpd_gps.php` copies `fudge1`, `fudge2`, `refid` from POST with no CR/LF reject. Stratum is the only numeric check. `write_config` then `configd_run('service restart ntpd')`. PPS is the sibling for `fudge1` / `refid`.

`ntpd_configure_do` then, only after a successful GPS configure, concatenates:

```php
$ntpcfg .= 'fudge 127.127.20.0';
if (!empty($config['ntpd']['gps']['fudge1'])) {
    $ntpcfg .= ' time1 ';
    $ntpcfg .= $config['ntpd']['gps']['fudge1'];
}
```

Same shape for `fudge2` and `refid`. Timeservers got `str_replace(["\n", "\r"], '', $ts)`. These fields did not. Result is written to `/var/etc/ntpd.conf`. ntpd is started as the configure UID, which is root via configd. No `user` directive is emitted.

The GPS/PPS fudge block is emitted only when configure_gps/pps returns true, so an existing `cua*` char node is required (onboard `cuau0` or a USB callout is the usual case). NTP must be enabled.

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

06 Wrong turns, in order

I first walked 53581 as a keep. The path is now an allowlist of `/dev/cua*` char devices. Operator bar said DROP 53581 if the path is allowlisted. It is. Then I looked at h793 XSS. Medium. No root chain. Then I assumed fq94 had covered every ntpd.conf interpolation. Timeserver hosts yes. GPS fudge no. Then I looked at `custom_options`. Already `userIsAdmin`. Then I wondered whether a missing serial node closed the leftover. It closes the fudge block emit. A box with a serial console or a USB GPS still emits it. That is not rare.

07 The lab

PHP 8.3 gadget of pinned `ntpd_configure_do`. `mknod /dev/cua0`. Interpolation of GPS fudge stays in the unmodified pin copy. Loopback identity `127.0.0.1:18830`. Compose project `opnsense-ntp-gps-fudge`. ntpd is not started.

CONTROL: timeserver host with CR/LF. Collapsed to one token. `timeserver-stripped=yes`. TRIGGER: GPS `fudge1` CR/LF. Extra `logfile /oracle/OPNSENSE-NTP-GPS-FUDGE-WITNESS` after `fudge 127.127.20.0`. `fudge-newline=yes`.

Last run:

PLAIN TEXT Copy

```
SUCCESS opnsense-ntp-gps-fudge fudge-newline=yes timeserver-stripped=yes OPNSENSE
```

PPS sibling and live ntpd as root stay inferred. Honor of `includefile` / `driftfile` / `statsdir` stays inferred. Gadget, not a full OPNsense VM.

08 What an attacker can do

METHOD	SINK	PRIVILEGE
GPS `fudge1` CR/LF	pin `ntpd_configure_do` extra `logfile /oracle/OPNSENSE-NTP-GPS-FUDGE-WITNESS` after `fudge 127.127.20.0`	**Integrity (lab-proven):** ntpd.conf extra line. Lab: `fudge-newline=yes`.
honor of `includefile` / `driftfile` / `statsdir`	ntpd as root, no `-u`	**Integrity (inferred):** extra ntpd policy / file write at an

METHOD	SINK	PRIVILEGE
		ntpd-writable path. ntpd not started in the gadget.
timeserver host CR/LF	`ntpd.inc:327-329` strip	**Negative (lab-proven):** timeserver collapsed to one token. `timeserver-stripped=yes`.
PPS `fudge1` / `refid` CR/LF	PPS `fudge 127.127.22.0` block	**Integrity (inferred):** same class. Gadget ran the GPS path.
invalid extra directive	ntpd start	**Availability (inferred):** ntpd can fail to start.
this path	none	**Recon:** no extra read of `config.xml` secrets.

Requires: `page-services-ntp-gps` (lab) and/or `page-services-ntp-pps`. Not `page-all`. Live `/dev/cua*` char node. NTP enabled. CSRF token.

09 Adjacent surface that stays closed

CVE-2026-53581 arbitrary-path overwrite (`../` no longer leaves `/dev/`). GHSA-h793 GPS XSS (no chain). Timeserver host CR/LF (stripped). `custom_options` on the general NTP page (`page-all` only). Unauth.

10 The fix

Strip CR/LF (and treat quotes) on GPS/PPS `fudge1` / `fudge2` / `refid` the same way timeserver hosts already do at `ntpd.inc:327-329`. Or constrain those fields to a numeric / token class. Keep extra ntpd.conf text behind `userIsAdmin`.

Replay:

PLAIN TEXT Copy

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

Loopback `127.0.0.1:18830`. Witness `OPNSENSE-NTP-GPS-FUDGE-WITNESS`.

11 References

- Pack: github.com/abraxas/opnsense-ntp-gps-fudge
- Product: github.com/opnsense/core `a842fe48c21288d11a422cb944678e8eb308becf`
- `ntpd.inc`
- `services_ntpd_gps.php`
- Named fields (not this leftover): GHSA-fq94 timeserver host; CVE-2026-53581

serial path

- CWE-93 / CWE-74

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