0-DAY NO CVE HIGH PUBLIC

pfSense limiter hidden number into dnctl delete

pfSense CE 2.9.0-DEVELOPMENT Traffic Shaper Limiters emit a hidden number field on edit. Create overwrites it. Edit concatenates GetNumber() into dnctl pipe delete unquoted. Limited GUI user gets root. Labbed.

NAME pfSense limiter hidden number into dnctl delete	TYPE 0-day analysis
CVE n/a	CVE RISK high
DISCLOSURE STATUS public	VENDOR Netgate
AFFECTED pfSense CE 2.9.0-DEVELOPMENT (9363ac5) shaper.inc delete_queue / GetNumber. Privilege page-firewall-trafficshaper-limiter. Apply path is a file, not a shell.	PUBLISHED 13 Oct 2026
UPDATED 13 Oct 2026	TAGS 0-day, pfsense, limiter, rce, cwe-78

01 Hidden fields are still POST. Create already knew that.

I am @abraxas_null. The proof of concept is on GitHub: **abraxas/pfsense-limiter-number** (loopback client). The lab stack is `lab/`: Dockerfile, docker-compose.yml, run.sh, poc.py, gadget.php. Authorized lab only. It talks to loopback.

This is **pfSense CE 2.9.0-DEVELOPMENT** (`9363ac5b8651a1c7a333180425ce7719070f95f9`). No CVE yet. CWE-78. 8.8 High (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H`). Remote authenticated RCE. Privilege `page-firewall-trafficshaper-limiter`. Not Diagnostics: Command.

Create overwrites `number` with `dnpipe_find_nextnumber()`. Child create overwrites with `dnqueue_find_nextnumber()`. Edit does not. The existing limiter form emits a hidden `number` when `GetNumber() > 0`. `validate_input` checks name charset, bandwidth, delay, scheduler/AQM keys. It does not check `number`. `GetNumber()` is concatenated unquoted into `dnctl pipe|sched|queue delete`. PHP `mwexec` is `/bin/sh -c`. WebGUI PHP-FPM is root.

Apply writes `GetNumber()` into `/tmp/rules.limiter` then `dnctl` of that path. Filename is not user-controlled. File body is dummynet language, not a shell. That path is closed as RCE. Edit-then-delete is not.

02 Why pfSense, and this pin

PHP-FPM is root. Public GitHub has no `RELENG_2_9_0`. I hunted master `9363ac5` (2.9.0-DEVELOPMENT) and dropped leftovers that match a public SA. Skip Plus. Skip SA-26_01 through SA-26_22 including SA-26_20 Kea JSON (the named cmd-exec on DHCP, not this limiter). Advisories: https://docs.netgate.com/advisories/index.html

Twenty hunts. filter/NAT/alias/shaper/VIP is where hidden `number` lived. AQM params into `/tmp/rules.limiter` are extra dummynet lines. Medium. Not this leftover.

03 How number leaves the form

Create:

```php
/* dnpipe_find_nextnumber() overwrites POST number */
```

Edit form:

```php
if ($this->GetNumber() > 0) {
    $section->addInput(new Form_Input(
        'number',
        null,
        'hidden',
        $this->GetNumber()
    ));
}
```

POST edit: `update_dn_data` → `ReadConfig` → `SetNumber($q['number'])` and `wconfig` writes `$cflink['number'] = $this->GetNumber()`. `read_dummynet_config()` reloads that number from config. GET delete runs `delete_queue()`:

```php
function delete_queue() {
    cleanup_dnqueue_from_rules($this->GetQname());
    foreach ($this->subqueues as $q) {
        $q->delete_queue();
    }
    shaper_dn_config_del($this->GetLink());
    mwexec("/sbin/dnctl pipe delete " . $this->GetNumber());
    mwexec("/sbin/dnctl sched delete " . $this->GetNumber());
}
```

Child: `mwexec("/sbin/dnctl queue delete " . $this→GetNumber())`. Limiter names are `^[a-zA-Z0-9_-]+$`. `GetNumber()` is not.

04 The lab

PHP gadget of pinned `ReadConfig` / `SetNumber` / `delete_queue`. PATH stub `w` is the oracle. `/sbin/dnctl` is `/bin/true` so apply-file is a file write, not host dummynet. Loopback `127.0.0.1:18840`.

CONTROL create: `ReadConfig` kept a poisoned number, `dnpipe_find_nextnumber()` overwrote to `1`, delete ran `dnctl pipe delete 1`, no witness. CONTROL apply: attacker number sat in `/tmp/rules.limiter` body; argv was `dnctl` of that path. TRIGGER edit: `SetNumber` from POST `number` then `delete_queue()` ran `dnctl pipe delete` concatenating `GetNumber()`, witness present.

Last run:

PLAIN TEXT Copy

```
SUCCESS PFSENSE-LIMITER-NUMBER create-overwrites=yes apply-file=yes edit-delete-e
```

Stack tears down on EXIT.

05 What an attacker can do

METHOD	SINK
Create a limiter, POST save with attacker `number`, then delete that limiter	`mwexec("/sbin/d pipe delete " . $this→GetNumber ( shaper.inc:382`

METHOD	SINK
Same root shell	host filesystem
Root shell or `dnctl` of attacker numbers	dummynet

Lab-proven vs inferred: create overwrite (no witness), apply-file path (dnctl of a file, no witness), and edit-delete exec (witness) are lab-proven. Filesystem recon is inferred from root PHP-FPM.

Requires: WebGUI session with `page-firewall-trafficshaper-limiter`. CSRF on POST save. Delete is GET `action=delete`.

06 Adjacent surface that stays closed

SURFACE	LAB
Create path	`dnpipe_find_nextnumber()` overwrites, `create-overwrites=yes`
Apply path	`dnctl` of `/tmp/rules.limiter`, filename not user-controlled, `apply-file=yes`
Limiter name charset	`^[a-zA-Z0-9_-]+$`
Unauth	closed
Diagnostics: Command	stays closed unless also granted

07 The fix

Int-cast `GetNumber()` before every `dnctl`. Ignore POST `number` on edit, or range-check it against the live dummynet id. Create already overwrites; make edit do the same.

Replay:

PLAIN TEXT Copy

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

Loopback `127.0.0.1:18840`. Witness `PFSENSE-LIMITER-NUMBER-WITNESS`.

08 References

- Pack: github.com/abraxas/pfsense-limiter-number

- Product: github.com/pfsense/pfsense `9363ac5b8651a1c7a333180425ce7719070f95f9`
- `shaper.inc` `delete_queue` / `GetNumber`
- `firewall_shaper_vinterface.php`
- CWE-78

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

© 2026 Abraxas Labs