Abraxas Labs
ABRAXAS

DARK LIGHT

Research / pfsense-ipsec-login-banner

0-DAY NO CVE HIGH PUBLIC

pfSense IPsec login_banner into charon start-scripts

pfSense CE 2.9.0-DEVELOPMENT dumps IPsec Mobile login_banner unquoted into strongswan.conf attr.28672. A Form_Input-safe banner can close attr/plugins and plant charon.start-scripts. Apply restarts charon, which popens that path. Labbed.

NAME pfSense IPsec login_banner into charon start-scripts	TYPE 0-day analysis
CVE n/a	CVE RISK high
DISCLOSURE STATUS public	VENDOR Netgate
AFFECTED pfSense CE 2.9.0-DEVELOPMENT (9363ac5) vpn_ipsec_mobile.php / ipsec_strongswan_confgen. Privilege page-vpn-ipsec-mobile. include prefix was not used.	PUBLISHED 13 Oct 2026
UPDATED 13 Oct 2026	TAGS 0-day, pfsense, ipsec, strongswan, rce, cwe-74

01 The widget is one line. strongSwan still ends an unquoted value on a brace.

I am @abraxas_null. The proof of concept is on GitHub: **abraxas/pfsense-ipsec-login-banner** (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-74. 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-vpn-ipsec-mobile`. Not IPsec advanced. Not Diagnostics: Command.

Login banner is stored with a length check only. HTML widget is `Form_Input` type text. POST can still carry braces. `ipsec_setup_strongswan()` writes it unquoted as `charon.plugins.attr.28672`. `ipsec_strongswan_confgen()` emits `key = {$value}` with no quoting. strongSwan settings syntax ends an unquoted assignment on `#`, `}`, or newline. `charon.start-scripts` is `name = path` executed when the daemon starts. Apply on that page is `strongswanrc restart`. Upstream charon `run_scripts()` uses `popen` on that path.

IPsec mobile `dns_domain` on this page already uses `is_domain()`. P1 `descr` XSS is SA-26_14. Values whose first eight characters are `include` print without a key. This leftover did not use that prefix.

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_14 P1 description XSS. Advisories: https://docs.netgate.com/advisories/index.html

Twenty hunts. OpenVPN/IPsec is where `login_banner` lived. OpenVPN wizard CRLF is a different leftover (server `config.ovpn`).

03 How a banner becomes start-scripts

Store:

```php
if (!empty(config_get_path('ipsec/client/login_banner'))) {
    $ssconf['charon']['plugins']['attr'][] = "# Login Banner";
    $ssconf['charon']['plugins']['attr']['28672'] =
        config_get_path('ipsec/client/login_banner');
}
```

On this pin, `plugins` is the last `charon` subsection. Inside `plugins`, `attr` is last when mobile clients are enabled. Inside `attr`, `28672` is last unless the same form also sets `save_passwd` or `pfs_group`. The mobile page owns those checkboxes.

A Form_Input-safe banner (no newlines) closes `attr` / `plugins` and opens `charon.start-scripts`. Dummy sections after that block absorb the three closers confgen still emits (`attr`, `plugins`, `charon`) so the file remains a valid settings tree. Apply always restarts (`vpn_ipsec_mobile.php` comment #4353, `ipsec.inc` `strongswanrc restart`). Reload would only `--reload-settings`.

04 The lab

Pinned `ipsec_strongswan_confgen` plus real `/usr/lib/ipsec/charon`. Loopback `127.0.0.1:18850`. Compose project `pfsense-ipsec-login-banner`.

CONTROL: banner `Welcome` stays inside `attr`, no `start-scripts`, no witness. TRIGGER: Form_Input-safe banner closes `attr` / `plugins`, opens `charon.start-scripts`. Real charon loaded that file and `popen`'d the start-scripts path (`charon=yes`).

Last run:

PLAIN TEXT Copy

```
SUCCESS PFSENSE-IPSEC-LOGIN-BANNER control-no-scripts=yes start-scripts=yes charo
```

Stack tears down on EXIT.

05 What an attacker can do

METHOD

POST `vpn_ipsec_mobile.php` save with `login_banner_enable` + a banner that closes `attr` /

Same popen

Invalid `strongswan.conf` or IPsec restart

```
METHOD
```

Lab-proven vs inferred: control-no-scripts, start-scripts in the generated conf, and real charon popen are lab-proven. Filesystem recon is inferred from that popen.

Requires: WebGUI session with `page-vpn-ipsec-mobile`. CSRF token. Save then Apply on the same page. Does not require `page-all`, `page-vpn-ipsec-editphase1`, or an IPsec raw-config textarea.

06 Adjacent surface that stays closed

SURFACE	LAB
Control banner `Welcome`	stays inside `attr`, no start-scripts
Unauth / CSRF without token	closed
OpenVPN `config.ovpn`	different leftover
P1 HTML XSS	SA-26_14 skip-list
`page-vpn-ipsec-editphase1`	not required
Diagnostics: Command	stays closed unless also granted

07 The fix

Quote / escape `login_banner` in `ipsec_strongswan_confgen`. Reject `}` `#` and newlines on save (the HTML widget is already a single-line `Form_Input`).

`is_domain()` already exists on this page for DNS domain; banner needs the same class of check.

Replay:

PLAIN TEXT Copy

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

Loopback `127.0.0.1:18850`. Witness `PFSENSE-IPSEC-LOGIN-BANNER-WITNESS`.

08 References

- Pack: github.com/abraxas/pfsense-ipsec-login-banner
- Product: github.com/pfsense/pfsense `9363ac5b8651a1c7a333180425ce7719070f95f9`
- `vpn_ipsec_mobile.php`
- `ipsec.inc`
- strongswan.conf `charon.start-scripts`
- 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