SERIES 0-DAY NO CVE HIGH PUBLIC

pfSense CE leftovers, part 1: the pin that is not RELEASE

People treat the pfSense WebGUI as admin-already-has-root. That is true for Diagnostics: Command. It is not true for a limited GUI user granted a single page. This is the map of 39 leftover interpolations on public GitHub master 9363ac5 (2.9.0-DEVELOPMENT), follow-up to five already published shells.

07 SERIES pfSense CE leftover interpolations

00 The pin
01 Shell interpolations
02 Conf breakouts
03 Config takeover
04 Files and portal
05 XSS and redirect
06 Chains

NEXT →
Phase 1: Shell interpolations

NAME	SERIES
pfSense CE leftovers, part 1: the pin that is not RELEASE	pfSense CE leftover interpolations
PHASE	TYPE
0 · The pin	0-day analysis
CVE	CVE RISK
n/a	high

DISCLOSURE STATUS	VENDOR
public	Netgate
AFFECTED	**PUBLISHED**
pfSense CE 2.9.0-DEVELOPMENT public GitHub master 9363ac5. 2.9.0-RELEASE PHP was not on the public tree.	15 Oct 2026
UPDATED	**TAGS**
15 Oct 2026	0-day, pfsense, netgate, rce, series

01 Admin already has root. Until they do not.

I am @abraxas_null. This is a map, not a sink write-up.

People treat the pfSense WebGUI as "the admin already has root." That is true for Diagnostics: Command. The privilege is `page-diagnostics-command`. It carries `standard-warning-root`. The page is `diag_command.php`. PHP `exec`s the box. Nobody should be surprised.

It is not true for a limited GUI user who was granted a single page. `isAllowedPage` sits on the URI. csrf-magic sits on POST. `Form_Select` is HTML only. PHP-FPM still runs as root. `exec` and `mwexec` are still `/bin/sh -c`. A wireless-edit grant is not a command-prompt grant. A wizard grant is not User Manager. A hidden uploadconfig grant is not Backup & Restore. The warning flag is the difference, and most of the leftover pages do not have it.

This series is 39 new leftovers on that model. They sit on public GitHub master `9363ac5b8651a1c7a333180425ce7719070f95f9`. `src/etc/version` is 2.9.0-DEVELOPMENT. They are not the five shells I already published. They are not the 2026 Security Advisories. They are not Plus. They are not packages. They are interpolations that the named-page fixes walked past.

I mailed Netgate. Packs are AGPLv3. No CVE numbers yet. 2.9.0-RELEASE PHP was not on the public tree, so every row here is Unknown on RELEASE.

02 How to read this

Seven pages. This one is the pin, the skip list, the privilege model, and the map. The next five split the 39 by class. The last one is how they compose. Skip to the family you care about if you already believe the WebGUI is more than Diagnostics: Command.

01 **Part 1 - The pin** (you are here). Privilege model. Skip list. Map of 39 leftovers plus the five already published.

02 **Part 2 - Shell interpolations**. `ifconfig` / `pfctl` / `dpinger` family.

03 **Part 3 - Conf breakouts**. Daemon conf CRLF and quote-close: php.ini, sshguard, mpd, Unbound, OpenVPN, crontab.

04 **Part 4 - Config takeover**. Wizard, uploadconfig, ACB, LDAP name, readonly restore, WOL GET.

05 **Part 5 - Files and portal**. Captive Portal file manager, nginx `maxprocperip`, `file://`, DynDNS cache path, voucher SQLi.

06 **Part 6 - XSS and redirect**. Seven XSS leftovers plus `$http_host` 301.

07 **Part 7 - Chains**. How they compose.

Labs are PHP gadgets of pinned sinks on loopback. Not a full CE box. Witness-only. No exploit payloads. Each leftover has its own GitHub pack under

github.com/abraxas. Replay is `./run.sh` against 127.0.0.1.

03 Why this product

I wanted a large FreeBSD firewall with a PHP WebGUI and a privilege table that pretends a page is not the host. pfSense CE is that product. The GUI is Apache-2.0 PHP on FreeBSD. Netgate ships Plus as paid. CE is the public tree. The WebGUI is how operators actually touch the box.

The security model is consistent once you look at it:

- WebGUI PHP-FPM is **root**.
- `guiconfig.inc` loads `authgui.inc` `session_auth()`, then `isAllowedPage(REQUEST_URI)`.
- csrf-magic wraps POST except a short `$nocsrf` list.
- Session cookie is SameSite=Strict, HttpOnly, after `session_auth` sets the params.
- PHP `exec` / `mwexec` is `/bin/sh -c`. There is no argv array on the leftover paths.
- A limited user can be granted one MATCH glob without `page-diagnostics-command`.
- `Form_Select` renders an allowlist in HTML. It does not re-validate POST.

That last point is the class. VLAN edit already membership-checks a parent. QinQ edit did not. Wireless clone stores `$_POST['if']` with no allowlist. Assign Add stores `if_add` without `$portlist`. The widget looked like a dropdown. POST is a string.

Unauth WebGUI is closed on this pin. csrf-magic plus SameSite=Strict still blocks a foreign-site POST. Diagnostics: Command is intended. xmlrpc `exec_php` / `exec_shell` after HA Basic is intended for the HA principal; the unpublished uid-skip on that path is a public SA. I needed pages that are not warned as root and still concatenate into a shell, a daemon conf, or `config.xml`.

04 The pin that is not RELEASE

Public GitHub has no `RELENG_2_8_x` and no `RELENG_2_9_0`. Tags stop at v2.5.2. Latest public RELENG is `RELENG_2_7_2`. Actual latest stable CE is **2.9.0-RELEASE** (2026-08-20, config rev 24.6). PHP for that release is not on public GitHub. SA fix SHAs named in the advisories 404 on the public repo. I did not extract RELEASE PHP.

I pinned public master `9363ac5` (2026-03-31, Encode RSS widget post titles, fixes #16770). `src/etc/version` is 2.9.0-DEVELOPMENT. Config rev on that tree is 24.5. I dropped any leftover that matches a public SA even when the fix landed after this commit.

RELEASE column for every unpublished row is **Unknown**. The 2.9.0 notes name SA-25_09 and SA-26_01 through SA-26_21 as fixed. They do not name QinQ parent-if, wireless clone, timezone into php.ini, wizard uid 0, or the rest of this map. Tickets that *are* on this DEV pin do not close the siblings: #16128 is PPP **client** `get_mpd_str()`, already here, and does not touch L2TP/PPPoE **server** RADIUS. #16637 is Unbound General Settings checkconf merge, already here, and does not cover Advanced `sock_queue_timeout` or ACL name/action.

Treat this series as a public-tree audit. If RELEASE patched a helper, some siblings close. If RELEASE patched only the named page, they do not. I cannot tell from GitHub.

05 The skip list is half the hunt

docs.netgate.com/advisories already named a 2026 crop. I did not rediscover those bugs and I did not keep them because they are still in this tree.

- **SA-26_01** `isvalidpid` on this pin is already `posix_kill` plus an integer PID. Closed here.
- **SA-26_06** proxyuser/proxypass crontab CRLF. Skip. PPPoE `ptpid` crontab is a sibling leftover, different file.
- **SA-26_07** OpenVPN `vpn_openvpn_server.php` `dns_domain` / `netbios_scope`. Named page only. The wizard is a sibling I already published. `connect_async` eval and learn-address CN are different leftovers.
- **SA-26_18** dashboard widget sequence LFI. Skip.
- **SA-26_20** Kea custom JSON. Skip. ISC `dhcpd.conf` filename is a different leftover.
- **SA-26_22 / CVE-2026-92182** xmlrpc LDAP/RADIUS uid skip. Still in this tree. Affects CE <= 2.9.0. Public. Skip. WebGUI name collision with local `admin` is a different bug.
- **SA-26_04** RSS widget title XSS is the last commit on this pin. Body and permalink are leftovers. SimplePie `file://` redirect is a leftover.
- **SA-25_09** sshguard WebGUI brute-force. Different sshguard bug. `THRESHOLD` CRLF `BACKEND=` is a leftover.
- **SA-26_02** through **SA-26_21** otherwise: XSS / info-disclosure named pages. Skip even when a sibling field is still raw.

Plus is paid. Out. Packages that are not in this tree are out. In-tree miniupnpd was in scope and did not produce a KEEP I wanted to lab. Historical GIF/GRE parent-if is

CVE-2023-42326. QinQ did not get the existence check. That one is already public from the first wave.

Intended root stays intended: `diag_command.php`, xmlrpc `exec_php` / `exec_shell`, pfSsh `eval`, warn-root User Manager / Backup / auth servers, OpenVPN Advanced `custom_options`, documented Captive Portal PHP inside the portal jail, documented Custom DynDNS HTTP(S) URLs.

06 Five leftovers already on the table

The first hunt was Critical/High only. Twenty surfaces. Five independent PHP-gadget labs. Those five are **not** this series' 39. They are already public. I am not reprinting the sinks here.

LEFTOVER	PRIVILEGE	PACK	BL
QinQ parent-if into `ifconfig`	`page-interfaces-qinq-edit`	pfsense-qinq-parent-if	/re qi
OpenVPN wizard CRLF leftover of SA-26_07	`page-pfsensewizardsubsystem`	pfsense-openvpn-wizard-crlf	/re op cr
CARP VHID leftover into `ifconfig`	`page-firewall-virtualipaddress-edit`	pfsense-carp-vhid	/re ca
Limiter hidden `number` into `dnctl` delete	`page-firewall-trafficshaper-limiter`	pfsense-limiter-number	/re lin
IPsec `login_banner` into charon start-scripts	`page-vpn-ipsec-mobile`	pfsense-ipsec-	/re ip

LEFTOVER	PRIVILEGE	PACK	BL
		login-banner	

The dedicated cmd-injection hunt returned NONE and walked past QinQ. The interfaces hunt named the parent-if. CSC CRLF dropped as High because OpenVPN 2.6 CCD does not run `up`. Captive Portal `maxprocperip` dropped as High on that first pass because the shown breakout was portal availability. The second hunt put it back as leftover 22: labbed extra `location` / `alias` on the portal vhost. Host RCE still not shown.

07 Any-severity, forty labs

The second hunt dropped the High-only bar. Any unpublished leftover. Remote first. XSS is Medium unless it is on the unauth captive-portal origin. Daemon conf that is not a shell stays Medium. CSRF GET mutators stay Low or Medium. Privilege leftover that replaces `config.xml` without `standard-warning-root` is High even when it never calls `/bin/sh`.

Forty gadget labs. Thirty-nine SUCCESS. One FAIL.

The FAIL is `status_logs_filter_dynamic.php` `logfile` before the allow-list. Confused-deputy `cat` as root PHP is real. The AJAX serializer drops `message`, so the planted witness never appears in the body. I am not inflating that into a secret leak. It is not in the map. It is not a pack. It is the lab that told the truth and sat down.

The 39 SUCCESS rows are this series. Each one has a CONTROL, a TRIGGER, a witness file, and a last line that starts with `SUCCESS`. I am not going to paste those last lines here. Parts 2 through 6 do the sinks. This page is the index.

Unauth Critical unpublished: **none** on this pin. I looked. The HTTP-to-HTTPS 301 is an open redirect, not RCE. Captive Portal filename XSS needs a plant from the file

manager. `maxprocperip` needs a plant from the portal page. WOL GET needs a session cookie. That is the unauth surface I actually have.

08 The privilege model

`priv.defs.inc` is the table of record. A privilege is a name, a MATCH glob, and optionally `warn = standard-warning-root`. The warning is UI. It is not a second ACL. `isAllowedPage` does not read it. The operator who grants `page-interfaces-wireless-edit` is not shown the same banner as Diagnostics: Command.

Intended root, warned:

PRIVILEGE	MATCH	WARN-ROOT
`page-diagnostics-command`	`diag_command.php*`	yes
`page-diagnostics-backup-restore`	`diag_backup.php*`	yes
`page-diagnostics-configurationhistory`	`diag_confbak.php*`	yes
`page-diagnostics-edit`	`diag_edit.php*`	yes
`page-system-usermanager`	usermanager	yes
`page-system-authservers`	auth servers	yes
`page-openvpn-server-advanced`	OpenVPN advanced textarea	yes
`page-all`	everything	yes

Leftover pages, not warned. Limited user. Same root PHP-FPM.

PRIVILEGE	TYPICAL LEFTOVER	WARN-ROOT
`page-interfaces-wireless-edit`	wireless clone `ifconfig`	no

PRIVILEGE	TYPICAL LEFTOVER	WARN-ROOT
`page-interfaces-assignnetworkports`	Assign Add `if_add`	no
`page-interfaces-vlan-edit`	VLAN parent ioctl	no
`page-system-gateways-editgateway`	IPv6 zone into dpinger	no
`page-system-generalsetup`	timezone into php.ini	no
`page-system-advanced-admin`	sshguard `BACKEND=`	no
`page-vpn-vpnl2tp`	L2TP RADIUS into mpd	no
`page-services-pppoeserver-edit`	PPPoE mpd.secret `!`	no
`page-interfaces-ppps-edit`	PPPoE crontab	no
`page-services-captiveportal-hasync`	HA host into `pfctl`	no
`page-services-captiveportal-filemanager`	path write / portal XSS	no
`page-pfsensewizardsubsystem`	setup wizard uid 0	no
`page-hidden-uploadconfiguration`	POST `config=` install	no
`page-services-acb`	ACB `newver` restore	no
`page-services-dnsresolver-advanced`	Unbound sock-queue-timeout	no
`page-services-dnsresolver-acls`	Unbound ACL CRLF	no
`page-system-usermanager-passwordmg`	collision writes uid 0 hash	no
`page-services-dynamicdnsclient`	`file://` / cache path	no
`page-firewall-rules`	GET `if=` XSS	no

PRIVILEGE	TYPICAL LEFTOVER	WARN-ROOT
`page-services-wakeonlan`	GET `wakeall`	no

Default admin has every page. The leftover is the limited user. Grant wireless-edit. Do not grant Diagnostics: Command. PHP is still root. That is the whole model, compressed.

`isAdminUID` is the other half. A remote WebGUI login whose name equals local `admin` is not a stub. `getUserEntry($name)` returns the local row. Then:

```php
if ($user['uid'] == 0) {
    return true;
}
```

Loose compare. `isAllowedPage` short-circuits. Every page, including `diag_command.php`. passwordmg is not warn-root and treats the session as local. Stub-only remote names still fail closed. SA-26_22 is xmlrpc uid *missing*. This is WebGUI name *collision*. Different bug.

09 What an attacker can do

This is the series-level picture, not every sink.

A WebGUI session with one leftover page, a csrf-magic token, and POST (or a GET mutator where the page still honors `$_REQUEST`) is enough to reach that page's sink as root PHP. The operator who granted the page thought they granted a form. They granted the host.

Shell interpolations (`ifconfig`, `pfctl`, `dpinger`, OpenVPN `eval` / `su -c`) are host commands. Daemon conf breakouts (php.ini `auto_prepend_file`, sshguard `BACKEND=`, mpd `up-script` / `!` helper, Unbound `include:`, crontab extra line) are

host commands on the next restart or the next session. File write as root PHP is host RCE on this platform. Captive Portal file manager walking out of `cpelements` is that class.

Config takeover pages are not Diagnostics: Command. Wizard step 7 rewrites the uid 0 hash. Hidden `uploadconfig.php` `config_install`s a blob and reboots. ACB `newver` restores a listed revision. `user-config-readonly` stops `write_config` and does not stop `config_install` / `config_restore`. LDAP/RADIUS `admin` becomes `isAdminUID`. Those pages replace the device. They do not need a semicolon in an interface name.

XSS in the GUI origin can drive further POSTs as the victim. csrf-magic is same-origin. SameSite=Strict does not block a script that already runs in the GUI origin. Captive Portal filename XSS is the portal origin, not the GUI origin. It can read `auth_user` / `auth_pass` on that login page. It does not steal GUI cookies.

Unauth on this pin does not get a root shell. The 301 uses `$http_host` before PHP DNS-rebind. That is an open redirect. WOL GET wakes stored MACs if the browser already has a session cookie.

I am not going to write a production recipe. Parts 2 through 6 are witness labs. Part 7 is composition, still analysis-level.

10 The map

Thirty-nine leftovers. Class is the leftover class. Reach is Remote unless noted. Method is the short version. GitHub is the AGPLv3 pack. Part is where the sink is written up.

#	LEFTOVER	CLASS	REACH	METHOD	PACK
1	wireless clone parent into ifconfig	RCE	Remote	POST `if` stored raw; `wlan create wlandev` interpolates the base	pfsens wireles clone

#	LEFTOVER	CLASS	REACH	METHOD	PACK
2	Assign Add `if_add` plus unanchored `wireless_regex`	RCE	Remote	Add stores a non-`$portlist` name; GET `interfaces.php?if=optN` clones it	pfsens assign
3	IPv6 link-local zone into dpinger	RCE	Remote	`is_ipaddrv6` strips `%zone` and never charset-checks it; `start_dpinger` interpolates monitor	pfsens ipv6-z
4	timezone into php.ini `auto_prepend_file`	RCE	Remote	timezone POST not allowlisted; `rc.php_ini_setup` interpolates `date.timezone`	pfsens timezo phpini
5	sshguard.conf THRESHOLD CRLF BACKEND	RCE	Remote	numeric knobs not `is_numericint`; extra `BACKEND=` is the executable	pfsens sshgua
6	L2TP/PPPoE server RADIUS secret into mpd.conf	RCE	Remote	quoted but unescaped secret; extra `set iface up-script`; `get_mpd_str` is client-only	pfsens radius
7	PPPoE periodic-reset crontab	RCE	Remote	hidden `ptpid` not int; `configure_cron` writes fields raw	pfsens pppoe
8	PPPoE mpd.secret username bang helper	RCE	Remote	username charset allows CR/LF; mpd `!` is an external password helper	pfsens pppoe secret
9	Captive Portal HA host into pfctl	RCE	Remote	`backwardsyncip` not `is_ipaddr`; unquoted	pfsens ha-pfc

#	LEFTOVER	CLASS	REACH	METHOD	PACK
				`pfctl -a {$anchor}/{$host}`	
10	Captive Portal file manager path write	File write	Remote	name containing `captiveportal-` skips the prefix; `../` walks out of cpelements	pfsens filema write
11	LDAP/RADIUS WebGUI name collision with local admin	Privilege leftover	Remote	`getUserEntry` returns the local uid 0 row; `isAdminUID`; passwordmg writes the hash	pfsens ldap-n collisio
12	setup wizard leftover resets uid 0	Privilege leftover	Remote	`wizard.php?xml=setup_wizard.xml` step 7 `local_user_set_password`; MATCH has no warn-root	pfsens wizard
13	hidden uploadconfig leftover	Privilege leftover	Remote	POST `config=` → `config_install` → reboot; IDENT has no warn-root	pfsens uploac
14	Auto Config Backup restore leftover	Privilege leftover	Remote	`newver` decrypts and `config_restore`; local backup pages are warn-root	pfsens restore
15	Unbound sock-queue-timeout CRLF include	RCE	Remote	field stored raw; no `test_unbound_config` on Advanced; CRLF adds `include:`	pfsens unbou sock-t
16	Unbound ACL name/action CRLF include	RCE	Remote	same `include:` class, different typed field, still no checkconf	pfsens unbou crlf

#	LEFTOVER	CLASS	REACH	METHOD	PACK
17	OpenVPN `connect_async` eval of RADIUS username	RCE	VPN user	`eval` pfctl anchor with username; local GUI charset rejects it; RADIUS skips that check	pfsens ovpn- conne
18	OpenVPN learn-address CN as unbound	RCE	VPN cert	unquoted CN into `su -m unbound -c`; gated on Register OpenVPN clients	pfsens ovpn-l cn
19	Custom DynDNS / Check IP `file://`	File read	Remote	no HTTP-only `is_URL`; no `CURLOPT_PROTOCOLS`; body returned on match miss	pfsens dyndn
20	RSS widget SimplePie `file://` redirect	File read	Remote	direct `file://` rewritten; 3xx `Location: file:///` is `file_get_contents` as root	pfsens file-re
21	Captive Portal filename stored XSS	XSS	plant GUI, victim portal	filename into `<img src>` / CSS `url()` on default login HTML; GUI list encoded	pfsens filenan
22	Captive Portal `maxprocperip` nginx server block	Config injection	plant GUI, then unauth portal	integer check is on unused `maxproc`; extra `location` / `alias` accepted	pfsens maxpr
23	`status_logs_filter` resolve JSON as text/html	XSS	Remote	`json_encode` with no `JSON_HEX_TAG`; default Content-Type text/html	pfsens logs-fi xss
24	`firewall_rules` GET `if` reflected XSS	XSS	Remote	`value="<?=$if?>"` and JS string when `requirefirewallinterface` is on	pfsens rules-i

#	LEFTOVER	CLASS	REACH	METHOD	PACK
25	RSS item body / permalink leftover of 26_04	XSS	Remote	title encoded; body is `strip_tags` only; permalink is raw href	pfsens body-x
26	firewall separator color into `class=`	XSS	Remote	order-store copies color with no whitelist; text is encoded	pfsens separa color-x
27	LDAP/RADIUS session username XSS in `head.inc`	XSS	Remote	logout title interpolates `$_SESSION['Username']` raw; local charset rejects the trigger	pfsens auth- usern xss
28	crash_reporter textarea of `/var/crash` blobs	XSS	Remote	PHP error log is encoded; crash blobs are not	pfsens crash- report
29	`user-config-readonly` vs `config_install`	Privilege leftover	Remote	Deny Config Write stops `write_config`; restore still replaces `config.xml`	pfsens config reador restore
30	HTTP-to-HTTPS 301 uses `$http_host`	Open redirect	Unauth HTTP	nginx 301 before php-fpm; PHP DNS-rebind never runs	pfsens https-l redirec
31	bsnmpd syslocation quote/semicolon	Config injection	Remote	extra `read :=` community line; no include/exec without a planted `.so`	pfsens bsnmp
32	NTP GPS/PPS fudge/refid/stratum	Config injection	Remote	extra ntpd language; `mwexec` argv is the conf path	pfsens gps-fu
33	IGMP Proxy type	Config injection	Remote	POST `type` has no enum; extra `phyint` line	pfsens igmp-t

#	LEFTOVER	CLASS	REACH	METHOD	PACK
34	ISC dhcpd.conf filename	Config injection	Remote	`filename "..."` with no `addslashes`; Kea JSON is SA-26_20 skip	pfsens dhcpd
35	limiter AQM into `rules.limiter`	Config injection	Remote	extra dummynet line on apply; apply argv is the file path, not a shell	pfsens limiter-
36	DynDNS cache path uses `escapeshellarg` as a filename	File write	Remote	Custom host skips `is_domain()`; `/` still splits the path; content is `IP|epoch`	pfsens dyndn cache-
37	`voucher_expire` SQLite WHERE	SQLi	Remote	concatenates voucher into WHERE; unauth login path uses `escapeString`	pfsens vouch expire-
38	VLAN parent not in `$portlist`	ioctl leftover	Remote	save checks `does_interface_exist` only; `escapeshellarg` so not shell	pfsens vlan-p ioctl
39	Wake-on-LAN all devices GET	CSRF	session GET	`$_REQUEST['wakeall']` without `usepost`; #16961 is notes-only on this public tree	pfsens get-all

Limiter AQM (35) is extra dummynet language. Limiter hidden `number` into `dnctl delete` is already public and is not this row. VLAN parent ioctl (38) is not QinQ parent-if. QinQ had no existence check. VLAN has the existence check and skips `$portlist`. Different leftover.

11 Labs are gadgets, not a box

Every pack is the same shape. A PHP 8.3 gadget of the pinned function. PATH stubs for `ifconfig` / `pfctl` / `dpinger` / `unbound` / `mpd` / `sshguard` so the oracle is a witness file, not host networking. Docker Compose on loopback. `run.sh` brings the stack up, hits CONTROL, hits TRIGGER, prints one `SUCCESS` line, tears down on EXIT.

I did not stand up a full CE firewall. Witness-only means the extra `w` wrote `PFSENSE-*-WITNESS` through `/bin/sh -c`, or the generated conf contained the extra stanza, or `config.xml` was replaced. That is a claim about the interpolation, not about WAN exposure or a production data plane. Ports ran 18910 through 19300, one leftover each. First-wave labs used 18810-18850. None of those listeners should exist after `run.sh` exits.

12 Adjacent surface that stays closed

Unauth WebGUI RCE: none. Stub-only remote names: `isAdminUID` fail-closed. GIF/GRE name regex: closed. LAGG members: `does_interface_exist` plus `escapeshellarg`. VLAN missing parent: rejected. OpenVPN local Database charset: rejects the `connect_async` trigger. PPP client `get_mpd_str` and Unbound General Settings checkconf: already on this pin. RSS titles: encoded here. Captive Portal file-manager list encodes the same filename the portal HTML does not. Diagnostics: Command stays closed unless leftover 11 made the session `isAdminUID`. The rest of the tree that returned NONE stays NONE.

13 How they compose, briefly

Full chains are part 7. Two paragraphs so the map is not a pile of disconnected rows.

XSS in the GUI origin (logs filter JSON as HTML, rules `if=`, separator `class=`, RSS body, crash reporter, LDAP username in `head.inc`) can drive POSTs as the logged-in victim. csrf-magic is a same-origin token. A limited user who cannot see wireless-

edit can still be the browser that submits it if an admin is the XSS victim. That is the usual GUI XSS story. It is not new. It is why Medium XSS stays in the series.

Config takeover pages are not Diagnostics: Command. Wizard, uploadconfig, and ACB restore replace `config.xml` from privileges that User Manager and Backup already warn as root. File write as root PHP is host RCE on this platform: Captive Portal file manager walking to `/` is that write. LDAP name `admin` becomes `isAdminUID` and then the session *is* Diagnostics: Command, without that page ever being granted. Those are the joins. The rest is one page, one sink, one witness.

14 Coordinated, no CVE yet

I mailed Netgate on this pin. First wave 13 Oct 2026, this batch after. Packs are AGPLv3 (GNU Affero GPL v3.0). No CVE numbers yet. Please request them per leftover if they split. I will not invent a RELEASE column. If a helper was escaped in RELENG, some of these close. If only the named SA page was touched, they do not.

Part 2 starts with wireless clone. VLAN already asked. QinQ already answered. The clone path is the same class on a different form.

15 References

- Product: github.com/pfsense/pfsense `9363ac5b8651a1c7a333180425ce7719070f95f9`
- Version: `src/etc/version` 2.9.0-DEVELOPMENT
- Privileges: `priv.defs.inc`, `priv.inc`
- Advisories: https://docs.netgate.com/advisories/index.html

- 2.9.0 notes: https://docs.netgate.com/pfsense/en/latest/releases/2-9-0.html
- First wave: QinQ, OpenVPN wizard, CARP VHID, limiter number, IPsec banner

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

07 SERIES **pfSense CE leftover interpolations**

00 **The pin**
01 **Shell interpolations**
02 **Conf breakouts**
03 **Config takeover**
04 **Files and portal**
05 **XSS and redirect**
06 **Chains**

NEXT →
Phase 1: Shell interpolations

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