Security Audit — 020

Push It / Hub Controls / smack-back.php Attack Surface Review

Date: 2026-05-31
Release: 0.7.192 "Push It Real Good"
Auditor: Claude (Cowork session)

New Attack Surface Introduced This Release

1. smack-push-it.php — Hub-Side Fleet Settings Push

What it does: Hub admin page that pushes settings key/value pairs to all connected spoke sites via outbound cURL POST to `spoke/api.php?route=multisite/settings/push`.

Controls in place:

- Requires admin session via core/auth-smack.php ✓
- Hub guard: redirects to dashboard if multisite_role !== 'hub' ✓
- CSRF: validated with hash_equals() before any POST handler executes ✓
- SSL: CURLOPT_SSL_VERIFYPEER => true + CURLOPT_SSL_VERIFYHOST => 2 ✓
- Spoke URLs sourced from snap_multisite_nodes (DB, not user input) ✓
- Spoke API keys sourced from snap_multisite_nodes (DB, not user input) ✓

Residual risks:

- **SSRF via compromised DB:** If an attacker gains write access to snap_multisite_nodes they can inject an arbitrary URL and trigger an outbound cURL POST from the hub. Mitigated by: SSL verification enforced (can't easily hit internal non-HTTPS services), auth token is per-spoke (attacker also needs the spoke's API key). Severity: **Low** (requires prior DB write access).
- **Settings blast:** A hub admin can push any key from snap_settings to spoke snap_settings. The push group definitions in $push_group_keys limit what gets pushed per button click, but the underlying multisite/settings/push endpoint accepts arbitrary keys. Not exploitable from the UI; would require crafting a direct POST. Severity: **Info**.

2. hub_controls_* Settings Flags — Spoke-Side Trust Model

What it does: Hub pushes `hub_controls_[group] = '1'` alongside settings. Spoke stores these in snap_settings and smack-settings.php / smack-back.php check them to lock UI sections.

Controls in place:

- Spoke only accepts pushed settings from authenticated hub API calls (Bearer token) ✓
- Locking is UI-only — the underlying DB values are simply not overwritten on save ✓
- Spoke can verify hub connection status via its Multisite Management page ✓

Residual risks:

- **Hub compromise propagates to fleet:** A compromised hub admin account can push arbitrary settings to all spokes, and lock spokes out of changing those settings. This is by design (hub authority over fleet)

but is worth noting: hub admin credential hygiene is critical. Recommend 2FA on hub admin account.

• **Stale lock after hub disconnect:** If a spoke disconnects from the hub, hub_controls_* flags remain set in snap_settings. Spoke settings remain locked until a hub admin clears the flags (no automatic unlock on disconnect). **Action recommended:** add unlock-on-disconnect logic to the multisite/disconnect endpoint, or add a manual "Release Hub Control" button on the spoke's settings page.

3. smack-multisite-settings.php — Pre-existing CSRF Gap (Fixed This Release)

What it was: CSRF tokens were rendered in all push forms but hash_equals() was never called in the POST handlers. Any authenticated admin could be CSRF'd into pushing settings to all spokes.

Fix applied: `$csrf_valid = hash_equals($csrf, $_POST['csrf'])` computed once at top of POST handling; all handlers gated on it.

Verification: All three POST branches (save_dl_spokes, push_smackback, generic push_groups loop) now require $csrf_valid. ✓

4. smack-back.php — Rename of smack-smackback.php

No new attack surface. Auth guard, CSRF on all forms, no SSRF, no user-controlled file paths. Old URL (smack-smackback.php) is a 301 redirect stub — it does not bypass the breach lockout gate because core/auth-smack.php exempts only smack-back.php now.

Verification: `$_smack_exempt = ['smack-back.php', 'smack-update.php']` in core/auth-smack.php. ✓

5. Admin Theme Manifests — include $manifest_path

What it does: smack-globalvibe.php discovers assets/adminthemes/*/ directories and includes each [slug]-manifest.php. Manifest files return PHP arrays.

Risk: If an attacker could write a file to assets/adminthemes/[slug]/[slug]-manifest.php, they could execute arbitrary PHP. Path is constructed from directory basename, not user input.

Mitigations: File write access to assets/adminthemes/ requires server-level compromise (same risk level as writing any PHP file). No new exposure beyond existing PHP execution model.

Severity: Info (pre-existing category, no change from prior releases).

Summary Table

Issue	Severity	Status
smack-push-it.php missing SSL verify	**High**	Fixed
smack-push-it.php missing hub guard	**Medium**	Fixed
smack-multisite-settings.php CSRF theater	**Medium**	Fixed
SSRF via compromised snap_multisite_nodes	**Low**	Accepted
hub_controls stale lock after disconnect	**Low**	Open

Hub compromise propagates to fleet	**Info**	Accepted
Admin theme manifest include()	**Info**	Accepted

Recommended Follow-Up

1. **Auto-unlock hub_controls on spoke disconnect** — multisite/disconnect endpoint should zero out all hub_controls_* flags when a spoke removes itself from the hub.
2. **2FA enforcement option for hub installs** — consider flagging in Network Settings if hub admin accounts lack 2FA enabled.