

021A — Hub/Spoke Attack Surface: Addendum

Date: 2026-06-04
Applies to: SnapSmack 0.7.203
Original audit: 021 — Hub/Spoke Attack Surface (2026-06-04)
Scope: Status update for Findings 012, F4, F5, F6, F7

This document amends audit 021. All findings listed below have been resolved. No new findings are introduced. The original audit document should be read alongside this addendum.

Finding 012 (Cross-reference) — install.php Step 5: Missing POST Guard

Severity: Medium
Status: **CLOSED — finding was in error**

The POST-only guard for Step 5 of the installer was present at line 1061 of `install.php` prior to this audit. The finding was raised in error. No remediation was required or applied.

Finding F4 — SMACKBACK Mode Downgrade via Hub Push

Severity: Medium
Status: **FIXED — 0.7.203**
File: `core/multisite-api.php`, `smack-back.php`

`core/multisite-api.php` now gates `smackback_mode` downgrades (lockout → alert) via the same pending-confirmation mechanism used for `smackback_enabled = 0`. When a hub pushes a mode downgrade, the value is stored as `smackback_hub_pending_mode` and held for local admin approval. The spoke's SMACKBACK page displays an APPROVE / REJECT prompt. The downgrade does not take effect until the spoke admin explicitly confirms it locally.

Finding F5 — `hub_controls_*` Keys Never Delivered to Spokes

Severity: Medium
Status: **FIXED — 0.7.203**
File: `core/multisite-api.php`

All six `hub_controls_*` keys have been added to the `settings/push` allowlist in `core/multisite-api.php`:

- `hub_controls_timezone`
- `hub_controls_akismet`
- `hub_controls_ai`
- `hub_controls_smackback`
- `hub_controls_comments`
- `hub_controls_email`

Previously these keys were pushed by the hub but silently discarded on the spoke, meaning spoke setting-lock UI never activated. Spoke locking is now functional end-to-end.

Finding F6 — AI Key Push Silently Fails

Severity: Low
Status: **FIXED — 0.7.203**
File: `core/multisite-api.php`

`ai_provider`, `ai_key_claude`, `ai_key_gemini`, and `ai_key_openai` have been added to the `settings/push` allowlist. Hub AI key distribution to spokes now functions as designed.

Finding F7 — No Single-Owner Warning on Spoke Connection Page

Severity: Low
Status: **CLOSED — warning already present**
File: `smack-multisite.php`

`smack-multisite.php` displays a security notice at the spoke registration step, before the user generates a token:

"Only connect to a hub you personally own and control. The hub will have admin-level access to this site — including the ability to push settings, deploy updates, and trigger maintenance mode. Never connect to a hub operated by a third party."

The finding is satisfied. No code change was required.

All findings in audit 021 are now resolved. This addendum is the final status record for that audit.