

Security Audit — 025 “Skin JS Outside the Manifest”

Date: 2026-06-17 **Auditor:** Cowork session (Claude, Opus 4.8), for Sean **Severity:** Medium (integrity-posture bypass — not a direct injection) **Status:** Remediated for AURORA and The Grid this session; skin-wide audit flagged as follow-up.

1. The protocol

SnapSmack’s security posture requires that **all skin JavaScript load through the CMS manifest** — declared in a skin’s `require_scripts` and resolved against the registry in `core/manifest-inventory.php`. Skins are to carry **zero direct `<script>` tags**. This is what keeps every executable asset on a known, inventoried load path (the same inventory SmackBack file-integrity monitoring is built around). A direct `<script>` tag emitted from skin PHP sidesteps that inventory entirely.

2. The breach

Both shipping Grid-family skins emitted skin JS with direct `echo '<script ...>'` calls in `skin-footer.php`, bypassing the manifest:

Skin	Files loaded by direct <code><script></code> echo	Registered in inventory?	In <code>require_scripts</code> ?
AURORA	<code>aa-modal.js</code> , <code>au-lightbox.js</code> , <code>aurora-bg.js</code> , <code>aurora-wave.js</code> , <code>au-grid-reveal.js</code>	No	No
The Grid	<code>tg-modal.js</code> (redundant), <code>tg-lightbox.js</code>	<code>tg-modal</code> yes / <code>tg-lightbox</code> no	No

The Grid is the origin of the pattern; AURORA inherited it when it was cloned from The Grid, and this session’s `au-grid-reveal.js` added one more instance before it was caught.

Two secondary defects surfaced from the same root cause:

- **Cross-skin load.** AURORA’s `require_scripts` listed `smack-grid-nav` and `smack-grid-modal`, whose inventory paths are hardcoded to **The Grid’s** `tg-nav.js` / `tg-modal.js`. AURORA was therefore loading another skin’s engines (wrong `.tg-` namespace — silently inert) while its real modal/lightbox arrived only via the bypassing echoes.
- **Dead engine.** Because of the above, AURORA’s own `au-nav.js` was never loaded — its profile-aware sticky-nav (mini-avatar reveal) was non-functional.

3. Impact

The scripts are first-party, same-origin static assets, so this is **not** an injection or external-code-execution finding. The exposure is **loss of the integrity-monitoring guarantee**: executable JS shipped outside the inventory the posture promises covers “all skin JS,” so tampering with those files would not be seen by the manifest-based controls the way an inventoried file would. It is also a correctness/trust gap (cross-skin loading, dead nav). Rated **Medium** as a control bypass, not a live web-facing vulnerability.

4. Remediation (this session)

File	Change
<code>core/manifest-inventory.php</code>	Registered <code>smack-grid-lightbox</code> (<code>tg-lightbox</code>) and six AURORA engines: <code>smack-aurora-bg</code> / <code>-wave</code> / <code>-modal</code> / <code>-lightbox</code> / <code>-nav</code> / <code>-reveal</code> .

File	Change
<code>skins/aurora/manifest.php</code>	<code>require_scripts</code> now references AURORA's own <code>smack-aurora-*</code> handles; dropped the inherited <code>smack-grid-nav / smack-grid-modal</code> . v1.0.13.
<code>skins/aurora/skin-footer.php</code>	Removed all five direct <code><script></code> echoes; JS now loads via the <code>require_scripts</code> loop only.
<code>skins/the-grid/manifest.php</code>	Added <code>smack-grid-lightbox</code> to <code>require_scripts</code> . v1.3.20.
<code>skins/the-grid/skin-footer.php</code> both <code>skin-footer.php</code>	Removed both direct <code><script></code> echoes. Loader now busts skin-owned script paths on the skin version (and keeps defer), so manifest-loaded skin JS still cache-busts on a skin bump.

Post-edit EOF markers verified on `manifest-inventory.php` and both footers.

5. Follow-ups (flagged, not done here)

S1 — Skin-wide sweep. [Med] Every other skin must be checked for the same direct-`<script>` pattern and for inherited `smack-grid-*` handles in `require_scripts`. Any skin cloned from The Grid likely shares both defects. Audit per skin with post-edit structure verification — **do not bulk-edit skins** (Photogram and The Grid are locked; treat accordingly).

S2 — Confirm monitoring coverage. [Low] Verify SmackBack's integrity baseline actually ingests the newly-registered skin JS paths now that they are in the inventory — registration is necessary but the baseline pickup should be confirmed on a real update.

S3 — Handle hygiene. [Low] `smack-grid-nav / smack-grid-modal` hardcode The Grid's file paths. Skin-specific engines should use skin-specific handles so a `require_scripts` copy/paste can't cross-load another skin's code (the root of the AURORA defect).

6. Verdict

Real posture bypass, now closed for the two affected skins; AURORA also regains its own (previously dead) nav engine. Net-positive. Ship with the AURORA 1.0.13 / The Grid 1.3.20 push. Track S1–S3 as separate work.