

Maintenance Mode: Anonymous Session Creation, Parse Error 500, and Multisite Stats Warning

Date:	2026-05-22
Files:	core/maintenance-gate.php, smack-maintenance.php, smack-multisite-stats.php
Severity:	Low (Finding 1) / Low (Finding 2) / Informational (Finding 3)
Status:	Fixed in 0.7.169

Summary

Three issues were identified during a review of the maintenance mode feature (introduced in 0.7.168) and the live site error log for foundtextures.ca. None of the issues permit unauthorized access or data exposure. Two are fixed defects (an unclosed PHP block causing a 500 on the admin maintenance page, and unnecessary session creation in the public maintenance gate); one is a PHP warning caused by an absent null-coalescing fallback in the multisite stats period selector.

Finding 1 — maintenance-gate.php: Anonymous Session Creation

Severity: Low Status: Fixed in 0.7.169

Description

The public-facing maintenance gate (core/maintenance-gate.php, introduced in 0.7.168) called `session_start()` unconditionally when maintenance mode was active. For any visitor without an existing session, this created a new PHP session file on disk and sent a Set-Cookie: PHPSESSID response header before the 503 holding page was rendered.

The session contained no data and the visitor was about to receive the holding page and leave. However, unconditional session creation for unauthenticated visitors has two minor adverse effects: (1) it fills the session save path with short-lived empty session files, increasing disk I/O on high-traffic maintenance windows; (2) it leaks the session name and cookie configuration to visitors who should receive no application-level cookies at all.

Affected Code (pre-0.7.169)

```
// Start session if not already active so we can check login state if (session_status()
=== PHP_SESSION_NONE) { session_start(); }
```

Fix

The gate now checks for an existing session cookie before calling `session_start()`. If no PHPSESSID cookie is present, there is no active session to resume and therefore no logged-in user to check — `session_start()` is skipped entirely.

```
// Resume an existing session to check login state – never create a new one // for
visitors who will just see the holding page. If no cookie exists, there // is no
logged-in session to check, so skip session_start entirely. if (session_status() ===
PHP_SESSION_NONE && !empty($_COOKIE[session_name()])) { session_start(); }
```

Finding 2 — smack-maintenance.php: Unclosed if Block (500 on Admin Page)

Severity: Low Status: Fixed in 0.7.169

Description

The REBUILD THUMBNAILS section of smack-maintenance.php used PHP alternative syntax (if (...): / else: / endif;) for its batch-continue conditional. The else: branch was never closed — the endif; was present for the adjacent REGENERATE ALL THUMBNAILS block but was missing for the REBUILD block. PHP reported "syntax error, unexpected end of file on line 902" and returned HTTP 500 on every request to the admin Maintenance page.

The 500 was visible from the error log on foundtextures.ca immediately after the 0.7.168 update was applied. The admin Maintenance page was entirely inaccessible. No data was exposed, but the error message in a misconfigured display_errors environment could reveal internal path information.

Affected Code (pre-0.7.169)

```
<?php if (!empty($asset_sync_has_more)): ?> <form> ... CONTINUE button ... </form> <?php  
else: ?> <form> ... REBUILD button ... </form> </div> <!-- *** missing endif before this  
close *** -->
```

Fix

Added the missing between the closing tag and the that closes the .box container, matching the pattern of the adjacent REGENERATE ALL THUMBNAILS block.

```
<?php else: ?> <form method="POST"> ... <button type="submit" ...>REBUILD</button>  
</form> <?php endif; ?> <!-- added --> </div>
```

Finding 3 — smack-multisite-stats.php: Undefined Array Key Warning

Severity: Informational Status: Fixed in 0.7.169

Description

The period selector on line 50 of smack-multisite-stats.php used the null-coalescing fallback (?? 30) correctly in the in_array() validation check, but omitted it in the ternary true branch where the validated value was cast and assigned. When the ?days= query parameter was absent (the normal case for a direct page visit), PHP emitted a "Undefined array key days" warning. No incorrect data was produced — PHP coerced the absent key to zero, which then failed the in_array() check and defaulted to 30 — but the warning appeared in the error log.

Affected Code (pre-0.7.169)

```
// $_GET['days'] used bare in the true branch: $period = in_array((int)($_GET['days'] ??  
30), [7, 30, 90, 180, 365, 0]) ? (int)$_GET['days'] // *** undefined when days absent ***  
: 30;
```

Fix

Applied the same ?? 30 fallback to the true branch so both reads are consistent:

```
$period = in_array((int)($_GET['days'] ?? 30), [7, 30, 90, 180, 365, 0]) ?  
(int)($_GET['days'] ?? 30) : 30;
```

Design Note — Mesh Roster Key Distribution

Severity: Informational (Design Tradeoff) Status: Acknowledged

During review of `core/mesh-helpers.php` and `core/multisite-api.php`, it was noted that `ms_build_roster()` includes `api_key_local` in the peer list delivered to all spokes on ping and `/peers/list`. The `api_key_local` is the key the hub presents when calling each individual spoke (hub→spoke auth). A spoke receiving the roster therefore holds the hub's authentication credential for every other spoke in the fleet.

This is intentional for mesh mode — peers need keys to call each other directly without routing through the hub. However, the blast radius of a single compromised spoke is the entire fleet: an attacker with spoke-level access could impersonate the hub against all sibling spokes.

Mitigation path (deferred): generate dedicated spoke-to-spoke keys distinct from hub-to-spoke keys during handshake, and distribute only those peer keys in the roster. This scopes a compromised spoke's lateral reach to peer-level operations rather than hub-level privilege. Not prioritised for the current fleet size but noted for future architecture review.

Findings 1–3 are fixed in release 0.7.169 "Chesterfield". The design note is acknowledged and deferred.