SECAUDIT 031 - Web-host cloud push (Google Drive / OneDrive) removed

SECURITY AUDIT / PUBLIC REMEDIATION RECORD

Date: 2026-06-29 **Severity:** High (stored broad-scope OAuth credentials on a shared web host) **Status:** REMEDIATED in 0.7.324 "Fluttershy" **Disposition:** Feature removed, not patched. Offloaded to the desktop tool.

Finding

SnapSmack shipped a "Cloud Backup" feature that pushed backup / recovery-kit archives from the **web host** to a user's **Google Drive** or **OneDrive**:

- `smack-cloud.php` - admin OAuth-link + push UI and the OAuth callback.
- `core/cloud-engine.php` - `SnapSmackCloudOAuth`: OAuth flow + resumable chunked

upload. Google scope `https://www.googleapis.com/auth/drive.file`.

To work unattended it stored a long-lived **refresh token** (and the OAuth client secret) server-side, in `snap_settings` (`google_*` / `onedrive_*` keys).

Risk

On a shared / commodity web host this is an unacceptable attack surface. A server compromise (or a malicious co-tenant, a leaked DB dump, a backup left world- readable, etc.) hands the attacker a refresh token with `drive.file` scope - enough to **read, overwrite, or delete the user's cloud files**, including the very backups they were trying to protect. The blast radius extends off our platform and onto the user's Google/Microsoft account. The web app holding broad, persistent third-party write credentials is a class of mistake common to large CMSes and one we explicitly do not want to repeat. (It would also routinely time out chunked uploads on a constrained shared host - a non-starter operationally as well as a security liability.)

Remediation (0.7.324)

1. **Deleted** `smack-cloud.php` and `core/cloud-engine.php` (removed, not

disabled - dead OAuth/upload code is itself attack surface).

2. **Removed the entry points:** the "Cloud Backup" sidebar item (`core/sidebar.php`)

and the "CONFIGURE CLOUD" button (`smack-backup.php`), replaced with a short note explaining the change.

3. **Self-heal on update** (`core/updater.php`): on every updater load, delete the

retired files if present and `DELETE` the stored OAuth creds/tokens (`google_client_id|secret|refresh_token`, `onedrive_*`, `cloud_last_*`). A previously-linked install therefore ends up with **no** Drive/OneDrive credentials on the server after updating - nothing left to steal.

Replacement / policy

Cloud upload is **desktop-tool-only** (SUYB / the batch poster), where the user's own credentials live on the user's own machine and never touch a shared server. Web-host backups remain available by **direct download** and **FTP**. Pushing to the cloud from SnapSmack on a web host is no longer permitted, for shared-resource and security reasons. Documented publicly on snapsmack.ca (Wotcha).