SERIES 0-DAY NO CVE CRITICAL PUBLIC

# Stirling-PDF v3.2.0 leftovers

Stirling-PDF v3.2.0 closed the H2 FILE_READ / CREATE ALIAS strings. CREATE OR REPLACE ALIAS still walks past validateSqlContent and RUNSCRIPT commits it. Processing-folder implied root is the whole ./storage tree, so ROLE_USER lists and overwrites another owner's stored PDFs.

03 SERIES Stirling-PDF v3.2.0 leftovers

00 Stirling-PDF 3.2.0, H2 CREATE OR REPLACE ALIAS leftover of GHSA-mrr8

00 The pin

00 Stirling-PDF 3.2.0, processing-folder implied storage root IDOR

← PREVIOUS
Phase 0: Stirling-PDF 3.2.0, H2 CREATE OR REPLACE ALIAS leftover of GHSA-mrr8

NEXT →
Phase 0: Stirling-PDF 3.2.0, processing-folder implied storage root IDOR

| NAME | SERIES |
|---|---|
| Stirling-PDF v3.2.0 leftovers | Stirling-PDF v3.2.0 leftovers |
| PHASE | TYPE |
| 0 · The pin | 0-day analysis |
| CVE | CVE RISK |
| n/a | critical |
| DISCLOSURE STATUS | VENDOR |
| public | Stirling-PDF |

| AFFECTED | PUBLISHED |
| --- | --- |
| **Stirling-PDF v3.2.0 (a7e593728dd9aa81e75318a949789d3c2e9ee754). Images stirlingtools/stirling-pdf:3.2.0 and 3.2.0-fat.** | **17 Oct 2026** |
| **UPDATED** | **TAGS** |
| **17 Oct 2026** | **0-day, stirling-pdf, leftover, h2, idor, remote** |

## 01 They banned CREATE ALIAS. They left OR REPLACE sitting in the middle.

A named GHSA is a fence. The leftover is whatever still walks around it.

I am abraxas. This is the series hub for two leftovers I labbed on Stirling-PDF **v3.2.0** (`a7e593728dd9aa81e75318a949789d3c2e9ee754`), posted as @abraxas_null. The images are `stirlingtools/stirling-pdf:3.2.0` and `3.2.0-fat`. Template `security.enableLogin` is true. Official compose and the README `docker run` set `SECURITY_ENABLELOGIN=false`, then `anyRequest().permitAll()`. `@EnableMethodSecurity` stays on, so class `@PreAuthorize("hasRole('ADMIN')")` still 403s anonymous. Default first admin is `admin` / `stirling`. Loopback witness labs. No shells.

v3.2.0 is the current GA. It closed the GHSA-mrr8 / CVE-2026-85714 `FILE_READ` / `CREATE ALIAS` / `CSVWRITE` strings. Direct `/api/v1/storage/files/{id}` is owner-scoped. Two handlers next to those patches did not get the lesson.

The leftover I would patch first is H2 import. A ROLE_ADMIN `.sql` whose denylist is supposed to stop Java aliases still creates one, because the regex never learned `OR REPLACE`. A later backup download contains the witness.

The two posts, in that order:

01 stirling-h2-import-leftover - `CREATE OR REPLACE ALIAS` leftover of GHSA-mrr8

02 stirling-storage-folder-idor - processing-folder implied `./storage` root

A third candidate, markdown WeasyPrint SSRF leftover of GHSA-ff33, **FAILED** in lab. OWASP java-html-sanitizer **20260924.2** drops every absolute `img src` (`http`, `https`, `data:`) before `SsrfProtectionService`. Oracle 0 hits. It is not a disclosed leftover.

Vendor intake is the GitHub Security Advisory tab or security@stirlingpdf.com. Unpaid. I am not opening a public issue on Stirling-Tools/Stirling-PDF. Packs are AGPLv3 under github.com/abraxas. Labs talk to loopback and print a witness.

## 02 Why this product

Stirling-PDF is the self-hosted PDF toolbox people actually docker-run. Merge, watermark, convert, store, import a backup. Ninety-thousand GitHub stars is not a security argument, but it is a lot of default H2 files sitting under `./configs`.

I wanted unpublished Critical or High on the current GA, remote preferred. SaaS (`app/saas`) is another tree. I did not file it. Ultra-lite with `DISABLE_ADDITIONAL_FEATURES=true` drops the proprietary controllers this series needs; the HIT images are fat plus login-on.

The security model is honest once you look at it. Template login is on. Advertised compose login is off. Method security does not follow the HTTP `permitAll`. Conversion APIs become anonymous on the README one-liner. Database import does not. Storage CRUD 403s when login is off. Processing folders, on fat, still take a disk path. That split is how leftovers hide after a named GHSA: the patch names one string, or one controller, and leaves the sibling.

## 03 How the pin was chosen

Latest GA. Tag v3.2.0. Peel is `a7e593728dd9aa81e75318a949789d3c2e9ee754`. Images `stirlingtools/stirling-pdf:3.2.0` and `3.2.0-fat`. I did not chase main. A leftover on a GA tag is a leftover someone can reproduce.

Labs use those images on 127.0.0.1. Replay is `./run.sh` in each pack. Fat, login-on, default H2, a witness string in a backup or a watermark stream.

## 04 The skip list is half the hunt

Before you look for leftovers, you write down what is already public so you do not "discover" a CVE with a press release. Sixteen published GitHub advisories on this tree plus one public n-day. I did not re-file:

- GHSA-mrr8-934j-4g8m / CVE-2026-85714 H2 RCE via `POST /api/v1/database/import-database`. Bare `CREATE ALIAS`, `FILE_READ(`, `CSVWRITE(` are denied. The leftover of that validator is OR REPLACE.
- GHSA-ff33-grr6-rmvp / CVE-2025-55161 markdown-to-PDF SSRF. Direct `img src` is the named fence. Nested `data:` SVG and 302 leftover **FAILED** in lab (OWASP 20260924.2). Not disclosed.
- GHSA-xw8v-9mfm-g2pm / CVE-2025-55150 HTML-to-PDF SSRF. Same sanitizer.
- GHSA-wccq-mg6x-2w22 / CVE-2026-27625 markdown ZIP traversal. `startsWith` holds.
- GHSA-3xxh-mm3g-c9w5 / CVE-2026-57485 pipeline `INTERNAL_API_USER` key. Operation allowlist holds.

- GHSA-3×7x-943g-269w AI create-pdf-from-html-agent skip-sanitizer.
- GHSA-pr4g-9qp2-g8j8 SVG-to-PDF Batik LFI. Closed on this pin.
- GHSA-76hv-h7g2-xfv3 office/file-to-PDF SSRF.
- GHSA-998c-x8hx-737r / CVE-2025-46568 URL-to-PDF WeasyPrint file read. Default-off. Sibling CVE-2026-71270 is public. Do not re-file.
- GHSA-xmhg-fv84-jgfc EML-to-HTML XSS. XSS-only is out of bar.
- GHSA-pp9g-47g3-f789 CSV formula injection.
- GHSA-3932-2rfq-87xm, GHSA-q5j3-4m5w-wp75, GHSA-rjjx-43g5-mp76, GHSA-qc47-qgh9-xj63, GHSA-9j55-gvf2-cqwv. Closed, Medium/Low, or XSS.

Public n-day, still unpatched on this pin, so it is not this series: issue #7628 `.fodt` / `.fods` bypass of `OfficeDocumentSanitizer`. Do not "discover" it.

Hunts that returned nothing in this bar: SVG/Batik, office/LibreOffice (the public fodt hole), URL-to-PDF (default-off), pipeline INTERNAL_API_USER, zip-slip, share-links (`publicAccess` never set), MCP (off; POST authenticated), ExternalApiCall (admin-stored base URL), PrintFile/ProcessExecutor (no shell), job file IDs (UUID + owner), webhooks (HMAC), JWT/API keys, Python engine (not in default image), config/admin mutation (`@PreAuthorize ADMIN`), workflow signing tokens, EML/ebook/CBZ.

## 05 Two leftovers, one pin

| # | PACK | REACH | CLASS | WHAT AN ATTACKER CAN DO |
|---|---|---|---|---|
| 1 | stirling-h2- | Remote ROLE_ADMIN, | H2 RUNSCRIPT | Import `CREATE OR REPLACE ALIAS … FOR "java.lang.…"` the denylist is |

| # | PACK | REACH | CLASS | WHAT AN ATTACKER CAN DO |
|---|---|---|---|---|
| | import-leftover | default H2 fat | leftover | supposed to stop. Backup download contains attacker SQL. Host `FILE_READ` / FileUtils `.pth` RCE stay inferred from GHSA-mrr8. |
| 2 | stirling-storage-folder-idor | Remote ROLE_USER, login-on fat | IDOR | Point a processing folder at `storage/<victimId>`, list that owner's PDFs, sweep them in place. Direct `GET /api/v1/storage/files/{id}` stays 403. |

H2 is first because it is the original Critical class, restored through a regex gap. Storage is second because the CRUD API learned `findByIdAndOwner` and the disk path next to it did not.

The markdown leftover is not a third row. WeasyPrint 70.0.0 still ran. The sanitizer stripped `src` first. Zero oracle hits is a FAIL, not a blog post.

## 06 How I labbed them

Two independent compose projects. Unique loopback ports. `stirlingtools/stirling-pdf:3.2.0-fat`, login-on. Witness strings in a backup `.sql` or a FlateDecode watermark stream. Stacks torn down.

- H2: 127.0.0.1:18152. Unauth import 401. Bare `CREATE ALIAS` 500. `CREATE OR REPLACE ALIAS` 200 `importIntoDatabaseSuccessed`. Backup `backup_202610172328.sql` 50432 bytes contains the witness.
- Storage: 127.0.0.1:18154. Victim `admin` id 1. Attacker `peeruser` id 3 `ROLE_USER`. Direct storage GET 403. `directory=storage/1` lists the UUID-prefixed PDF. Sweep add-watermark. Victim Range 206 / 3450 contains the witness.

Replay: clone the pack, `python3 *-Abraxas-Labs.py` or `cd lab && ./run.sh`.

## 07 Contact

abraxaslabs.tech · github.com/abraxas · @abraxas_null · abraxas.null@proton.me

03 SERIES Stirling-PDF v3.2.0 leftovers

00 Stirling-PDF 3.2.0, H2 CREATE OR REPLACE ALIAS leftover of GHSA-mrr8

00 The pin

00 Stirling-PDF 3.2.0, processing-folder implied storage root IDOR

← PREVIOUS
Phase 0: Stirling-PDF 3.2.0, H2 CREATE OR REPLACE ALIAS leftover of GHSA-mrr8

NEXT →
Phase 0: Stirling-PDF 3.2.0, processing-folder implied storage root IDOR

Independent research. Private analysis by arrangement. No ads. abraxas.null@proton.me · For defensive awareness and authorized testing only.

© 2026 Abraxas Labs