Zip Slip Path Traversal in Media Archive Import (CWE-22)

Critical **DavidMStraub** published **GHSA-m5gr-86j6-99jp** last week

Package

gramps-webapi (pip)

Affected versions

>= 1.6.0, <= 3.11.0

Patched versions

3.11.1

Description

Summary

A path traversal vulnerability (Zip Slip) exists in the media archive import feature. An authenticated user with owner-level privileges can craft a malicious ZIP file with directory-traversal filenames to write arbitrary files outside the intended temporary extraction directory on the server's local filesystem.

Details

When importing media archives as ZIP file, `MediaImporter._check_disk_space_and_extract()` in `gramps_webapi/api/media_importer.py` called `zipfile.extractall()` without validating ZIP entry names. Python's `zipfile` module does not sanitize entry names containing `../` sequences, allowing extraction to paths outside the target directory.

Only users with **owner permission** can upload media ZIP archives, so the biggest risk is for multi-tree deployments, where tree owners are distinct from server administrators.

For multi-tree deployments, the impact depends on deployment configuration. Assuming the standard docker-based deployment is used:

- **SQLite family tree + local media**: An attacker can overwrite another tree's database file or media files, leading to cross-tree data corruption or replacement.
- **Postgres family tree + S3 media**: No persistent tree data is stored on the local filesystem, so cross-tree impact is eliminated. The remaining risk is overwriting volume-mounted files such as the

application config file.

- **Postgres family tree + S3 media + environment-variable-only config**: No persistent files of value are present on the local filesystem. Impact is limited to writes to ephemeral container storage, which are lost on woker restart.

Fix

ZIP entry names are now validated against the resolved real path of the temporary directory before extraction. Any entry whose resolved path falls outside the temporary directory raises an error and aborts the import.

Severity

Critical 9.1 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	High
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	High
Availability	High

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

CVE ID

CVE-2026-40258

Weaknesses

▶ CWE-22

Credits

srisowmya2000 Reporter