Arbitrary file write via path traversal in file upload

High **lfnovo** published **GHSA-x4q2-89g5-594v** last month

Package

open-notebook

Affected versions

<= 1.8.3

Patched versions

1.8.4

Description

Description:

The file upload endpoint does not sanitize provided filenames. By intercepting the upload request and changing the filename to a path traversal payload (e.g., `../../../../tmp/test.txt`), an authenticated user can write files to arbitrary locations on the container filesystem.

Impact

- Write files to any path the application process can access
- Overwrite application code or configuration
- Write webshells to web-accessible directories

Patches

Fixed in v1.8.4. Filenames are now sanitized with `os.path.basename()` and the resolved path is validated to stay within the upload directory.

Credit

Reported by CERT-EU Offensive Security Team.

Severity

High 8.1 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

No known CVE

Weaknesses

▶ CWE-22