Arbitrary file read via Local File Inclusion in source creation

High **lfnovo** published **GHSA-842v-h4cj-r646** last month

Package

open-notebook

Affected versions

<= 1.8.3

Patched versions

1.8.4

Description

The `POST /api/sources` endpoint accepts a user-controllable `file_path` field. When `type=upload`, this path is passed directly to the content extraction pipeline without validating it is within the uploads directory. An authenticated user can specify arbitrary file paths (e.g., `/etc/passwd`, `/proc/self/environ`) and the file contents will be stored as a Source, readable through the UI.

Impact

- Read any file inside the Docker container
- Exfiltrate source code, configuration, and secrets
- Access `/proc/self/environ` for environment variables including the encryption key

Patches

Fixed in v1.8.4. The `file_path` is now validated to be within the uploads directory using `Path.resolve()` and `startswith()` checks.

Credit

Reported by CERT-EU Offensive Security Team.

Severity

High 7.7 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

No known CVE

Weaknesses

▶ CWE-22