Remote Code Execution via Jinja2 Server-Side Template Injection in transformations

Critical **lfnovo** published **GHSA-f35w-wx37-26q7** last month

Package

open-notebook

Affected versions

<= 1.8.3

Patched versions

1.8.4

Description

User-created transformation prompts are rendered by an unsandboxed Jinja2 `Environment` via the ai-prompter library. An authenticated user can inject Jinja2 template expressions (e.g., `{{cycler.__init__.__globals__.os.popen('id').read() }}`) to execute arbitrary Python code on the server.

Impact

- Remote Code Execution (RCE) on the Docker container
- Access environment variables including the encryption key used to decrypt stored API keys
- Read/write arbitrary files on the container filesystem
- Execute arbitrary system commands

Patches

Fixed in v1.8.4. The ai-prompter dependency was bumped to 0.4.0 which uses Jinja2 `SandboxedEnvironment` for all template rendering.

Credit

Reported by CERT-EU Offensive Security Team.

Severity

Critical 9.9 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

No known CVE

Weaknesses

▶ CWE-1336