Arbitrary File Read via Path Traversal in HTMLExporter Image Embedding

Moderate **minrk** published **GHSA-7jqv-fw35-gmx9** 9 hours ago

Package

nbconvert (pip)

Affected versions

>= 6.5,<7.17.1

Patched versions

7.17.1

Description

Summary

When `HTMLExporter.embed_images=True`, nbconvert's markdown renderer allows arbitrary file read via path traversal in image references. A malicious notebook can exfiltrate sensitive files from the conversion host by embedding them as base64 data URIs in the output HTML.

Patches

Upgrade to nbconvert 7.17.1

Workarounds

Do not enable `HTMLExporter.embed_images` (it is not enabled by default).

Severity

Moderate 6.5 / 10

CVSS v3 base metrics

Attack vector Network

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

Learn more about base metrics

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

CVE ID

CVE-2026-39378

Weaknesses

- CWE-22
- CWE-23

Credits

g0blinResearch Reporter