Arbitrary File Write via Path Traversal in Cell Attachment Filenames

Moderate **minrk** published **GHSA-4c99-qj7h-p3vg** 9 hours ago

Package

nbconvert (pip)

Affected versions	Patched versions
>= 6.5,<7.17.1	7.17.1

Description

Arbitrary File Write via Path Traversal in Cell Attachment Filenames

Summary

nbconvert allows arbitrary file writes to locations outside the intended output directory when processing notebooks containing crafted cell attachment filenames. The `ExtractAttachmentsPreprocessor` passes attachment filenames directly to the filesystem without sanitization, enabling path traversal attacks. This vulnerability provides complete control over both the destination path and file extension.

Impact

This vulnerability allows writing files with arbitrary content to arbitrary filesystem locations, limited only by the permissions of the process running nbconvert. The attacker controls:

- Full destination path (via `../` traversal)
- Filename
- File extension
- File content

Patches

- upgrade to nbconvert v7.17.1

Workarounds

disable ExtractAttachmentsPreprocessor by setting:

```
c. ExtractAttachmentsPreprocessor.enabled = False
```

Severity

Moderate 6.5 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-39377

Weaknesses

- CWE-22
- CWE-73

Credits

g0blinResearch Reporter