

CVE-2026-89065 and CVE-2026-89066: Issue with projen - Path traversal and OS command injection

Bulletin ID: 2026-108-AWS

Scope: AWS

Content Type: Important (requires attention)

Publication Date: 09/11/2026 09:00 AM PDT

Description:

projen is an open-source tool for defining and synthesizing software project configurations as code. AWS identified two issues in projen affecting the generated file manifest cleanup component and the task synthesis component.

- [CVE-2026-89065](#) — Relative path traversal in the generated file manifest cleanup component in projen before 0.101.37 might allow context-dependent attackers to recursively delete files and directories outside the project directory, via crafted entries in the version-controlled generated file manifest (.projen/files.json) that is consumed during project synthesis. The corrected containment check is automatically applied by the projen runtime the next time it is run.
- [CVE-2026-89066](#) — Improper neutralization of special elements used in an OS command in the task synthesis component in projen before 0.103.0 might allow context-dependent attackers to execute arbitrary commands on a developer workstation or continuous integration runner via shell metacharacters in project configuration values and repository file names that are interpolated into generated task definitions in .projen/tasks.json.

Impacted versions:

- All projen versions before 0.101.37 (CVE-2026-89065)
- All projen versions before 0.103.0 (CVE-2026-89066)

Resolution:

- **CVE-2026-89065** has been addressed in [projen version 0.101.37](#). Upgrading to 0.101.37 or later is sufficient; re-synthesis is not required.
- **CVE-2026-89066** has been addressed in [projen version 0.103.0](#). After upgrading, you must re-synthesize your project to regenerate .projen/tasks.json with the corrected task definitions. Upgrading alone is not sufficient because the generated task definition file is committed to the repository.



We recommend upgrading to the latest version and ensuring any derivative code is patched to incorporate the new fixes.

Workarounds:

- **CVE-2026-89065:** Review the version control history of .projen/files.json for entries that escape the project directory and remove them prior to running projen.
- **CVE-2026-89066:** Audit project configuration values — including LambdaFunctionOptions.entrypoint, AddBundleOptions fields, JestOptions.extraCliOptions, PytestOptions.testMatch, ReleaseOptions.artifactsDirectory, and other properties listed in the advisory — for shell metacharacters and remove or escape them prior to running projen.

References:

- [CVE-2026-89065](#)
- [GHSA-7p65-6x86-v7f3](#)
- [CVE-2026-89066](#)
- [GHSA-q6q4-h6vc-vqm8](#)

Please email aws-security@amazon.com with any security questions or concerns.

- Resources+
- Developers+
- Help+



Amazon is an equal opportunity employer and does not discriminate on the basis of protected veteran status, disability or other legally protected status. Veterans, military spouses, and people with disabilities are encouraged to apply.



Back to top ↑

