LangSmith SDK: Streaming token events bypass output redaction

Moderate **jkennedyvz** published **GHSA-rr7j-v2q5-chgv** last week

Package

langsmith (npm)

Affected versions	Patched versions
<=0.5.18	0.5.19

langsmith (pip)

<=0.7.30	0.7.31

Description

Summary

The LangSmith SDK's output redaction controls (hideOutputs in JS, hide_outputs in Python) do not apply to streaming token events. When an LLM run produces streaming output, each chunk is recorded as a new_token event containing the raw token value. These events bypass the redaction pipeline entirely — prepareRunCreateOrUpdateInputs (JS) and _hide_run_outputs (Python) only process the inputs and outputs fields on a run, never the events array. As a result, applications relying on output redaction to prevent sensitive LLM output from being stored in LangSmith will still leak the full streamed content via run events.

Details

Both JS and Python SDKs are affected. The same pattern exists in both:

- **JS SDK**: `traceable.ts:997-1003` and `traceable.ts:1044-1050`
- **Python SDK**: `run_helpers.py:1924` and `run_helpers.py:1996`

In both SDKs, `new_token` events with raw `kwargs.token` values are added during streaming, and the redaction pipeline (`hideOutputs` in JS, `hide_outputs` in Python) only processes `inputs` / `outputs` — never `events`.

Severity

Moderate 5.3 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-41182

Weaknesses

- CWE-200
- CWE-359
- CWE-532

Credits

 **Ryu7zz** Reporter