Tool execution result spoofing

Low **liqiang-fit2cloud** published **GHSA-f3c8-p474-xwfv** yesterday

Package

No package listed

Affected versions

<=v2.7.1

Patched versions

v2.8.0

Description

Summary

An authenticated user can bypass sandbox result validation and spoof tool execution results by exploiting early process termination and Python introspection. By calling sys.exit(0), an attacker terminates the execution wrapper before it prints the legitimate output, forcing the backend to accept a forged result written directly to standard output.

Details

MaxKB allows authenticated users to execute custom Python tool code. To securely extract the result from standard output and ignore any random print statements made by the user's tool, a temporary wrapper script is generated. This wrapper generates a random UUID (_id) interpolated directly into the script, executes the user's code, and then prints the _id followed by the JSON-encoded return value.

An attacker can write malicious code that: 1. Uses Python frame introspection (sys._getframe(1).f_code.co_consts) to read the hardcoded _id from the compiled bytecode constants of the generated wrapper script. 2. Constructs a forged JSON response and writes it directly to the system's standard output file descriptor 1 (os.write(1, payload)), bypassing the redirect_stdout(open(os.devnull, 'w')) context manager. 3. Immediately calls sys.exit(0) to terminate the python process successfully (return code 0).

Since the process terminates early, the legitimate wrapper lines that print the genuine _id and result are never reached. Therefore, the attacker's single forged line is the only line (and thus, the last line) that matches the _id prefix, successfully causing the MaxKB service to parse and trust the spoofed result.

Severity

Low 3.1 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-39419

Weaknesses

No CWEs