COMMUNITY CONTENT

Submit #782879: badlogic pi-mono 0.58.4 Unauthenticated Remote Code Execution

Title	badlogic pi-mono 0.58.4 Unauthenticated Remote Code Execution
Description	A critical unauthenticated remote code execution vulnerability exists in the @mariozechner/pi-mom Slack bot. Any member of the Slack workspace where the bot is installed can send a direct message or @mention to the bot, and the message content is passed directly to an LLM that has unrestricted access to a bash tool capable of executing arbitrary shell commands on the host system. The bot performs no application-level authentication or authorization — the only requirement is Slack workspace membership. The bash tool has no command filtering, no allowlist, no blocklist, and no human-in-the-loop confirmation. The default execution mode is host (no sandboxing), meaning commands run with the full privileges of the process running the bot. This is a true zero-interaction remote code execution: the attacker sends a Slack message, and the bot autonomously processes it, invokes the LLM, and executes whatever shell commands the LLM decides to run. The victim (bot operator) does not need to take any action.
Source	https://github.com/August829/CVEP/issues/28
User	Yu Bao (UID 88856)
Submission	03/19/2026 10:23 AM (17 days ago)
Moderation	04/04/2026 03:50 PM (16 days later)
Status	Confirmed
VulDB entry	[redacted] [badlogic pi-mono up to 0.58.4 pi-mom Slack Bot slack.ts authentication bypass]
Points	20

Community Content

Submissions are made by VulDB community users. VulDB is *not responsible* for their content nor the links to external sources.

Please use the raw information shown and the links listed *with caution*. They might contain malicious and harmful actions, code or data.

The corresponding VulDB entries contain the moderated, verified, and normalized information provided within the raw submission.

Documentation

- Submission Policy
- Data Processing
- CVE Handling