COMMUNITY CONTENT

Submit #782876: badlogic pi-mono 0.58.4 Zero-Click Remote Code Execution

Title	badlogic pi-mono 0.58.4 Zero-Click Remote Code Execution
Description	A code execution vulnerability exists in the extension loading mechanism of @mariozechner/pi-coding-agent. On startup, the agent automatically discovers and executes all TypeScript/JavaScript files found in the project-local .pi/extensions/ directory. The extension code is loaded via jiti.import() and its exported factory function is immediately invoked with full Node.js privileges — the same privileges as the user running the agent. No user confirmation, no trust prompt, no code signing verification, and no sandboxing is applied before execution. A malicious git repository containing a .pi/extensions/backdoor.ts file achieves arbitrary code execution the moment the victim runs pi in the cloned directory. The extension code executes during the startup phase, before the user sees any interactive prompt or has any opportunity to inspect the project configuration. This makes the vulnerability effectively zero-click after the initial pi command.
Source	https://github.com/August829/CVE-P/issues/27
User	Yu Bao (UID 88956)
Submission	03/19/2026 10:19 AM (17 days ago)
Moderation	04/04/2026 03:47 PM (15 days later)
Status	Published
VulDB entry	[badlogic pi-mono up to 0.58.4 loader.ts discoverAndLoadExtensions code injection]
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