

Switch 2 security takes a hit as hackers unlock homebrew access

A security researcher has demonstrated a software-only partial jailbreak of the Switch 2, gaining “userland” access that he says “lets us run homebrew, reverse engineer and mod Switch 2 games, back up save files off the Switch, and access most of the Switch 2’s peripherals through MMIO.”

The hack relies on the original Switch version of SmileBasic 4, the latest in a long-running series of programming environments and interpreters that run on Nintendo hardware. The so-called “tethered” hack also requires access to a macOS or Linux PC on the same network to run a node.js package that helps enable privileged system access.

Researcher Sammy Hajhamid writes that he used OpenAI’s Codex to poke at SmileBasic’s language interpreter, using a custom harness that could send USB commands to the system and view results via HDMI (as well as power cycling via a Bluetooth light switch flipping device). After “substantial effort for ~2 weeks,” that harness discovered a 32-bit integer overflow that occurs when removing items from an array in SmileBasic. That error gives access to an array pointer, which in turn allows read and write access to portions of system memory.

[Read full article](#)

Comments

<https://arstechnica.com/gaming/2026/10/switch-2-jailbreak-gives-hackers-new-ways-to-run-homebrew-and-mod-games/>