Hacking group says it has found encryption keys needed to unlock the PS5 [Updated]

By Kyle Orland

Published: 2021-11-08 · Archived: 2026-04-02 12:36:32 UTC

Hacking group Fail0verflow announced Sunday evening that it had obtained the encryption "root keys" for the PlayStation 5, an important first step in any effort to unlock the system and allow users to run homebrew software.

The tweeted announcement includes an image of what appears to be the PS5's decrypted firmware files, highlighting code that references the system's "secure loader." Analyzing that decrypted firmware could let Fail0verflow (or other hackers) reverse engineer the code and create custom firmware with the ability to load homebrew PS5 software (~~signed by those same symmetric keys to get the PS5 to recognize them as authentic~~).

[**Update (Nov. 9):** Aside from the symmetric encryption/decryption keys that have apparently been discovered, separate asymmetric keys are needed to validate any homebrew software to be seen as authentic by the system. The private portion of those authentication keys does not seem to have been uncovered yet, and probably won't be found on the system itself. Still, the symmetric keys in question should prove useful for enabling further analysis of the PS5 system software and discovering other exploits that could lead to the execution of unsigned code. Ars regrets the error.]

Extracting the PS5's system software and installing a replacement both require some sort of exploit that provides read and/or write access to the PS5's usually secure kernel. Fail0verflow's post does not detail the exploit the group used, but the tweet says the keys were "obtained from software," suggesting the group didn't need to make any modifications to the hardware itself.

Separately this weekend, well-known PlayStation hacker theFlow0 tweeted a screenshot showing a "Debug Settings" option amid the usual list of PS5 settings. As console-hacking news site Wololo explains, this debug setting was previously only seen on development hardware, where the GUI looks significantly different. But TheFlow0's tweet appears to come from the built-in sharing function of a retail PS5, suggesting he has also used an exploit to enable the internal flags that unlock the mode on standard consumer hardware.
