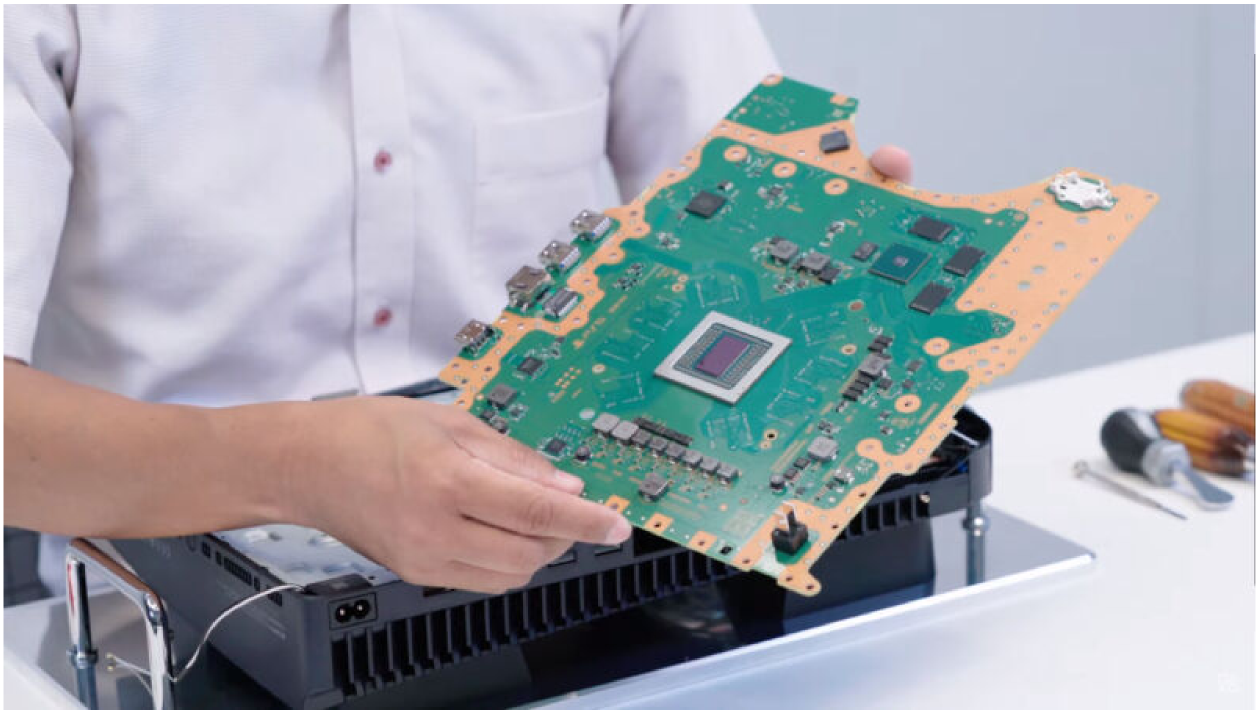
Hacking group says it has found encryption keys needed to unlock the PS5 [Updated]

ars arstechnica.com/gaming/2021/11/uncovered-ps5-encryption-keys-are-the-first-step-to-unlocking-the-console/

Kyle Orland

November 8, 2021



Enlarge / Decrypting the PS5 kernel doesn't involve opening the hardware like this, but it still serves as a good visual metaphor for how the system is now being "exposed."
Sony / YouTube

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.

TheFlow0 adds that he has "no plans for disclosure" of his PS5 exploit at this point. In recent years, TheFlow0 has taken part in Sony bug-bounty programs that reward the responsible disclosure of security flaws in PlayStation hardware.

A history of hacking

Further Reading

PS3 hacked through poor cryptography implementation

The weekend announcement from Fail0verflow comes roughly 11 years after the group announced that it had uncovered the private keys for the PlayStation 3 by taking advantage of a faulty cryptography implementation on Sony's part. Sony later sued members of the collective for what it said was circumventing the system's security; hacker George "GeoHot" Hotz discovered the same information independently and published the actual key on his website (the case was later settled). Back in 2013, Fail0verflow wrote a blog post suggesting that "we may have reached the point where homebrew on closed game consoles is no longer appealing," thanks in part to "a very real threat of litigation" and the fact that "game pirates would become not just big users of the result of those efforts, but by far the overwhelming majority (not because there are more pirates, but because there are fewer homebrewers)." But in 2018, Fail0verflow was one of a number of hacking groups that discovered the "unpatchable" exploit allowing unsigned code to run on the Nintendo Switch.

It remains to be seen if and when similar exploits for the PS5 will become public and if Sony will be able to temporarily cut them off with firmware updates as it has in the past.