New hack runs homebrew code from DVD-R on unmodified PlayStation 2



reader comments

35 with 28 posters participating

Share this story

[embedded content]
A demo from CTurt shows an SNES emulator running on a PS2 from a burned DVD-R.
Nearly 20 years after its initial release, a hacker has found a way to run homebrew software on an unmodified PlayStation 2 using nothing but a carefully burned DVD-ROM.

Previous efforts to hack the PS2 relied on internal modifications, external hardware (like pre-hacked memory cards and hard drives), or errors found only on very specific models of the system. The newly discovered FreeDVDBoot differs from this previous work by exploiting an error in the console's DVD

video player to create a fully software-based method for running arbitrary code on the system.

Security researcher CTurt laid out the FreeDVDBoot discovery and method in detail in a blog post this weekend. By decrypting and analyzing the code used for the PS2's DVD player, CTurt found a function that expects a 16-bit string from a properly formatted DVD but will actually easily accept over 1.5 megabytes from a malicious source.

Sending carefully formatted data to that function causes a buffer overflow that in turn triggers another badly written function to tell the system to jump to an area of memory with arbitrary, attacker-written code. That code can then tell the system to load an ELF file written to a burned DVD-R in the system. Building on previous PS2 homebrew efforts like uLaunchELF, it's relatively simple to use that DVD-R to load homebrew software or even full copies of otherwise copy-protected PS2 games.

The exploit is currently limited to very specific versions of the PS2's DVD player firmware (as of press time, firmwares 3.10 and 3.11, when set to "English") found in later editions of the console and won't work in earlier systems. But CTurt writes that he's "confident that all other versions also contain these same trivial IFO parsing buffer overflows" and can be exploited with broadly similar methods. The possibility of similar hacks through the Blu-ray player on the PS3 and PS4 (or the CD player on the PS1) are also being examined by the community.

Better late than early?

In the year 2020, a new software-only hacking method for the PS2 seems unlikely to have much effect on Sony's bottom line. But we can't help but marvel at how lucky Sony was that an exploit like this wasn't found and disseminated during the PS2's heyday in the early '00s.

[embedded content]
A DVD-R copy of *Shadow of the Colossus* running on an unmodified PlayStation 2, courtesy of Cturt's hack.
Remember, the PS2 existed in a day and age before regular system firmware updates were distributed via download or packaged on game discs. Thus, a PS2 exploit that allowed for simple, widespread piracy with nothing but a DVD burner could have had a huge impact on the market for PS2 software, much as similar exploits did for the Dreamcast and its legacy.

More than that, though, this new PS2 hack once again proves that even the best copy-protection schemes will eventually fall if the community puts in enough attention and effort. At best, console makers are just buying time before someone finds a way to trick the system into acting like an arbitrary computer. For Sony, it seems, their efforts bought them over 20 years of effective protection from simple, DVD-R-based hacks.

Listing image by CTurt / YouTube

https://arstechnica.com/?p=1688063