CD-indexing cue files are the core of a serious Linux remote code exploit

Enlarge / Cue files used to be much better-known, back when we all used CD-Rs to make legal backup copies of material that we owned outright.
Getty Images

reader comments

44 with

It has been a very long time since the average computer user thought about .cue files, or cue sheets, the metadata bits that describe the tracks of an optical disc, like a CD or DVD. But cue sheets are getting attention again, for all the wrong reasons. They're at the heart of a one-click exploit that could give an attacker code execution on Linux systems with GNOME desktops.

CVE-2023-43641, disclosed by GitHub on October 9, is a memory corruption (or out-of-bounds array writing) issue in the libcue library, which parses cue sheets. NIST has yet to provide a score for the issue, but GitHub's submission rates it an 8.8, or "High." While the vulnerability has been patched in the core library, Linux distributions will need to update their desktops to fix it.

GNOME desktops have, by default, a "tracker miner" that automatically updates whenever certain file locations in a user's home directory are changed. If a user was compelled to download a cue sheet that took advantage of libcue's

vulnerability, GNOME's indexing tracker would read the cue sheet, and code in that sheet could be executed.

- Part one of the .cue-based exploit example: An Ubuntu desktop, with a browser open, downloading a CUE file.
  Kevin Backhouse / GitHub
- Part 2: A calculator immediately pops up, with "1337" in the numerical display. You can imagine that most exploits would have far worse consequences.
  Kevin Backhouse / GitHub

Kevin Backhouse, a member of GitHub's Security Lab, offers a video demonstration of the exploit in his blog post but has not yet published the proof of concept to allow for patching. You can test your system's vulnerability against a test cue sheet he offers, which should trigger "a benign crash."

Advertisement

The bug is specific to how libcue reads the index of a disc track or its number and length. Because of the system tools it uses, you can trick libcue into registering a negative number for an index. Then, because another part of the scanning routine doesn't check whether an index number is negative before it writes it to an array, an attacker can write outside the array's bounds. Backhouse's proposed fix adds a single condition check to the index-setting routine.

Backhouse's blog post explains further how tracker-miners, like those in GNOME, are particularly vulnerable to this kind of exploit.

The current solution is for users of GNOME-based distributions to update their systems as soon as possible. The vulnerability in libcue is patched as of version 2.3.0. Libcue is typically a rather quiet project, maintained largely by Ilya Lipnitskiy alone. It illustrates, yet again, the vast amounts of technological infrastructure underpinned by tiny, unpaid projects.

This isn’t Backhouse’s first contribution to broad Linux vulnerabilities. He has previously found issues with standard users becoming root with a few commands and a Polkit exploit that also offered root access. Backhouse, despite being a recurring bearer of bad news, added this footnote to his most recent vulnerability disclosure: “I currently run Ubuntu 23.04 as my main OS and I *love* the GNOME desktop environment.”

https://arstechnica.com/?p=1975395