

Home » Posts

My 0-days in IObit

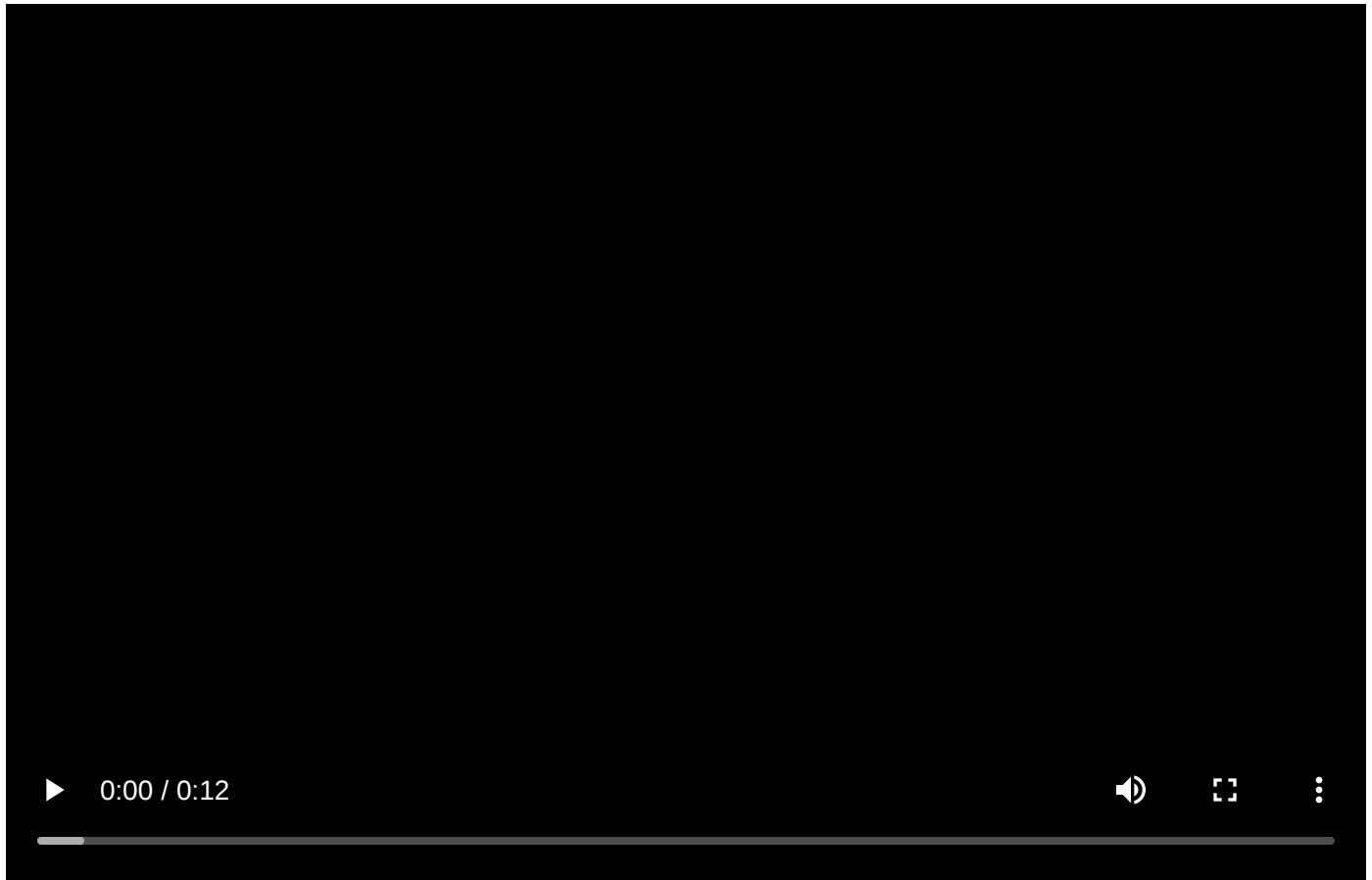
March 13, 2026 · 1 min · 143 words · Nathan

I've been doing some driver reverse engineering and exploitation since the last webserver. Since then, I have found 4 high severity CVE's in drivers or programs.

These all lead to privilege escalation from low/medium integrity -> high integrity. This product claims 10 million active users and 500 million downloads, thats hard to beleive though.

This shows two seperate privilege escalations in the same exact anti virus. Two entirely different methods, same result.

(ignore the sounds of the coffee in the background lol)



Here are my githubs for all of these local privilege escalation vulnerabilities:

[File Delete Vuln to LPE in AV - Awaiting CVE ID](#)

[DLL search issue in AV - CVE-2026-37333](#)

[IOBit unlocker driver bypass - CVE-2026-37334](#)

I was rewarded with a product code for these vulnerabilities.

[Ticket-YQRB-88309-2390]Advanced SystemCare FREE-Report a bug/error Inbox x



IObit Support
to me ▾

Hi there,

We can gift you one license code of our products as a thank-you gift for your report on this issue.

Please tell us which product you like.

--

Best regards,
IObit Support Team

Here was the professional writeup I sent that clearly explains all of the issues.

Writeup

« [PREV](#)

[NEXT](#) »

[ROP chaining, stack overflows, and OSED](#)

[Kernel only webserver \(rootkit\) with direct control of RIP pointer](#)