

[Acronis Advisory Database](#) > [Advisories](#) > [SEC-5487](#)

Published [3 years ago](#) • updated [10 days ago](#)

# Local privilege escalation due to insecure driver communication port permissions

HIGH SEVERITY

CVE-2023-41743

ACRONIS CYBER PROTECT 15

ACRONIS CYBER PROTECT CLOUD AGENT

ACRONIS CYBER PROTECT HOME OFFICE

ACRONIS TRUE IMAGE OEM

WINDOWS

@ALFAROM256

## Affected products

- Acronis Cyber Protect Home Office (Windows) before build 40278
- Acronis Cyber Protect Cloud Agent (Windows) before build 31637
- Acronis Cyber Protect 15 (Windows) before build 35979
- Acronis True Image OEM (Windows) before build 42575

## Updates

UPD-2512-8f77-a8c7 • published [4 months ago](#)

Acronis True Image OEM 2026 build 42575

ACRONIS TRUE IMAGE OEM

WINDOWS

UPD-2304-c825-6d96 • published [3 years ago](#)

Acronis Cyber Protect 15 update 6

ACRONIS CYBER PROTECT 15

LINUX

MACOS

WINDOWS

UPD-2302-3bd6-1ff4 • published [3 years ago](#)

Acronis Cyber Protect Home Office build 40278

ACRONIS CYBER PROTECT HOME OFFICE

WINDOWS

UPD-2302-5f99-5c6d • published [3 years ago](#)

Acronis Cyber Protect Cloud Agent update C23.02

ACRONIS CYBER PROTECT CLOUD AGENT

WINDOWS

MACOS

LINUX

## CVSS score

8.8 High

[CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H](#) 

## CWEs

- [CWE-269](#) 

## References

- [SEC-4858](#)

## Credits

- [@alfarom256](#) 

---

 [Contact us](#)

 [Report a vulnerability](#)

 [Subscribe to our Atom feed](#)

---

**Acronis** © 2003-2026 Acronis International GmbH.

