Product Security Advisory
2025T001
Several vulnerabilities in third party component Wibu Key

Affected Products

Product Name	Versions
All	All versions including and before v45

Vulnerability details

On November 13th 2025, several vulnerabilities were reported by Wibu Systems that may cause privilege scalation and denial of service. For further details check Wibu Systems provided documentation on the issue (here and here). **A fix is available** (see "Remediation" below).

Technical details:

- CVSS v3.1 base score: 8.8
- CVSS v3.1 vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
- Severity: high

Remediation

The remediation instructions below must be followed on all computers with Lantek software installed.

To fix the vulnerability, **update the Wibu Systems driver to version 6.71 or later**. To do so, download the driver from the Wibu Systems download page here, install it, and restart the computer afterwards.

Lantek Quality Assurance team has successfully tested this update in every release from v2020 and later.

Additional notes

- The vulnerability, as stated by Wibu Systems, **cannot** be exploited remotely. A malicious user needs to have local access to the computer to be able to exploit it successfully.
- In case you need to install or reinstall Lantek software on any computer, do not reuse any previously downloaded installers, because they could not have the latest security updates. As best practice, **we recommend always downloading the latest installers**. You can do so from the following links:

v45 SP1 METAL

v45 SP1 FACTORY

v44 SP1 METAL

v44 SP1 FACTORY

v44 SP1 SHARP

v43 SP2 FACTORY

METAL MTB SAPPHIRE

v43 SP2 METAL

v43 SP2 SHARP

V2022 SP1 METAL

V2022 SP1 FACTORY

V2022 SP1 SHARP

V2021 SP1 METAL

V2021 SP1 FACTORY

V2021 SP1 SHARP

V2020 SP1 METAL

Document revision history

Date	Author	Changes
November 18th, 2025	Lantek Cybersecurity Team	Initial relase