VECTOR

# Vector Keyman

**Important Security Information (last update: 2024-12-18)**

# WIBU CmDongle security vulnerablities

Following critical security vulnerabilities within WIBU CmDongle Firmware has been discovered lately.

| | |
|---|---|
| CVE-2024-45678 | A vulnerability has been found in a cryptographic library of Infineon Technologies that is part of their cryptocontroller embedded within the CmDongles. The exploitation of this vulnerability has been classified as complex: potential attackers need physical access to the device and require special equipment to exploit the vulnerability. In general, this vulnerability affects only ECC keys used to calculate signatures with the ECDSA algorithm. |

## Applicability to Vector Keyman

Vector Keyman is used as a cryptographical secured USB dongle to store Vector provided licenses for our product portfolio.
Vector Keyman is based on WIBU CmDongle including the CmDongle firmware which is affected by the security vulnerability. All firmware version < 4.52 are affected.

## Risk analysis

Risk analysis result: medium risk
Physical access to the device is needed for exploitation. The vulnerability cannot be exploited via network access.

## Recommended actions

Remediation:

- Update the firmware of the CmDongle to version 4.52 or newer.

CodeMeter Control Center can be used to update the firmware of Vector Keyman.
Please refer to WIBU Website **Security Advisories - Wibu-Systems** (**https://www.wibu.com/de/support/security-advisories.html**) for further information.

PLEASE NOTE: The vulnerability refers exclusively to the firmware of Vector Keyman based on WIBU CmDongles. Vector License container with PC as carrier (aka CmActLicenses), are NOT affected by the above-mentioned vulnerability.