TLP:WHITE

# VDE-2025-005: Phoenix Contact: Security Advisory for ESL Stick USB-A

| | |
|---|---|
| Publisher: Phoenix Contact GmbH & Co KG | Document category: csaf_security_advisory |
| Initial release date: Tue Jan 14 12:00:00 CET 2025 | Engine: 2.5.16 |
| Current release date: Tue Jan 14 12:00:00 CET 2025 | Build Date: Fri Jan 10 09:58:52 CET 2025 |
| Current version: 1 | Status: FINAL |
| CVSSv3.1 Base Score: 4.2 | Severity: medium |
| Original language: | Language: en-GB |
| Also referred to: VDE-2025-005, PCSA-2024/00019 | |

## Summary

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

## Impact

An attack would enable an attacker to create licenses that can be transferred into arbitrary CmDongles or CmActLicenses. A scaling hack is possible which can distribute licenses that cannot be distinguished from legitimate ones.

## Mitigation

Following measures are recommended to reduce the risk until the fixed version can be installed. Please be aware that not all mitigations apply to every possible product configuration, so please check which of these could be relevant or applicable in your case: As physical access is needed to exploit the vulnerabilities, it is recommended to take strict measures to control the access to the CmDongles, especially to the FSBs (Firm Security Box). General security best practices can help to protect systems from local and network attacks.

## Remediation

Update the firmware of the CmDongle to version 4.52. The FW for the CmDongle can be downloaded on the Wibu-Systems webpage.

## Product description

CmDongle for saving licenses for various software products.

# Vulnerabilities

## CVE-2024-45678

### Summary

Yubico YubiKey 5 Series devices with firmware before 5.7.0 and YubiHSM 2 devices with firmware before 2.4.0 allow an ECDSA secret-key extraction attack (that requires physical access and expensive equipment) in which an electromagnetic side channel is present because of a non-constant-time modular inversion for the Extended Euclidean Algorithm, aka the EUCLEAK issue. Other uses of an Infineon cryptographic library may also be affected.

| | |
|---|---|
| **CWE:** | CWE-203: Observable Discrepancy |
| **Release date:** | Tue Jan 14 12:00:00 CET 2025 |

## Product status

### Known affected

| Product | CVSS-Vector | CVSS Base Score |
|---|---|---|
| Firmware < 4.5.2 installed on ESL STICK USB A<br>Order number: 1080084 | CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N | 4.2 |

### Fixed

| Product |
|---|
| Firmware 4.5.2 installed on ESL STICK USB A<br>Order number: 1080084 (Download) |

# Acknowledgments

Phoenix Contact GmbH & Co KG thanks the following parties for their efforts:

- CERTVDE for Coordination
- Wibu-Systems for Reporting
- Infineon for Reporting
- NinjaLabs for Reporting

# Phoenix Contact GmbH & Co KG

Namespace: https://phoenixcontact.com/psirt

psirt@phoenixcontact.com

# References

- VDE-2025-005: Phoenix Contact: Security Advisory for ESL Stick USB-A - HTML (SELF): https://certvde.com/en/advisories/VDE-2025-005/
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://certvde.com/de/advisories/vendor/phoenixcontact/
- PCSA-2024/00019 (EXTERNAL): https://phoenixcontact.com/psirt
- VDE-2025-005: Phoenix Contact: Security Advisory for ESL Stick USB-A - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2025/vde-2025-005

# Revision history

| Version | Date of the revision | Summary of the revision |
|---|---|---|
| 1 | Tue Jan 14 12:00:00 CET 2025 | Initial revision |

# Sharing rules

**TLP:WHITE**

For the TLP version see https://www.first.org/tlp/