2024-11-22
Version 1.0

Product Security Advisory WIBU-100094

Vulnerability Title

Infineon ECDSA secret-key extraction attack

Affected products

Product name	Affected versions	Fixed Versions
CmDongle	CmDongles with an Infineon security cryptocontroller: CmSticks, CmCards and CmASICs with serial numbers starting with „3-“, e.g. 3-4380431.	Firmware version 4.52

PLEASE NOTE:

The vulnerability refers **exclusively** to the firmware of CmDongles.
CmCloudContainers and CmActLicenses are NOT affected by the above-mentioned vulnerability.
Physical access to the device is needed for exploitation. The vulnerability cannot be exploited via network access.

Vulnerability Description

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.

- CVE: CVE-2024-45678
- CVSS v3.1 Base Score: 6.8 (Medium)
  Note: the base score represents the reasonable worst-case scenario. Please check the scores section below to find the score that corresponds to your use case(s).
- CVSS v3.1 Vector: CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:N
- Vulnerability type:
  - CWE-203: Observable Discrepancy

CVSS v3.1 Scores

The CVSS Score depends on the stakeholder’s role: end user or ISV (software/device manufacturer).

CVSS v3.1 Scores for the end user:

- **No CmDongle**
  No risks for the end user
  /C:N/I:N/A:N No threats
  CVSS v3.1 Score: 0.0 None (vector: CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U**/C:N/I:N/A:N**)

- **No keys stored in Secret Data, Hidden Data or Universal Data**
  No risks for the end user
  /C:N/I:N/A:N No threats
  CVSS v3.1 Score: 0.0 None (vector: CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U**/C:N/I:N/A:N**)

- **ECDSA Keys stored in Universal Data (UvD)**
  Only ECDSA keys are affected. Other keys (AES, RSA) stored in Universal Data are not affected. The score depends on the sensitivity of the protected data, so it could be between **2.0 Low** and **4.9 Medium.**
  - **CVSS v3.1 Score: 2.0 Low** (CVSS:3.1/AV:P/AC:H/PR:N/UI:N**/S:U/C:L**/I:N/A:N)
  - **CVSS v3.1 Score: 4.9 Medium** (CVSS:3.1/AV:P/AC:H/PR:N/UI:N**/S:C/C:H**/I:N/A:N)

- **ECDSA, RSA or AES keys stored in Secret Data or Hidden Data**
  a) If the length of the keys is < 31 bytes:
  No risks for the end user
  /C:N/I:N/A:N No threats
  CVSS v3.1 Score: 0.0 None (vector: CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U**/C:N/I:N/A:N**)
  b) If the length of the keys is >= 31 bytes:
  The score depends on the sensitivity of the protected data, so it could be between **2.0 Low** and **4.9 Medium.**
  - **CVSS v3.1 Score: 2.0 Low** (CVSS:3.1/AV:P/AC:H/PR:N/UI:N**/S:U/C:L**/I:N/A:N)
  - **CVSS v3.1 Score: 4.9 Medium** (CVSS:3.1/AV:P/AC:H/PR:N/UI:N**/S:C/C:H**/I:N/A:N)

CVSS v3.1 Scores for the ISV (software/device manufacturer)

- **No CmDongle**
  No risks for the ISV
  /C:N/I:N/A:N No threats
  CVSS v3.1 Score: 0.0 None (vector: CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U**/C:N/I:N/A:N**)

- **No Universal Firm Code (Firm Code < 6.000.000)**
  No risks for the ISV
  /C:N/I:N/A:N No threats
  CVSS v3.1 Score: 0.0 None (vector: CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U**/C:N/I:N/A:N**)

- **Universal Firm Code (Firm Code > 6.000.000) and no License Transfer or Borrowing**
  An attacker could extract relevant keys from a license.
  /S:C/C:H The protected product is compromised. An Attacker with a valid license might create a cryptographic hack but is not able to create a valid license.
  CVSS v3.1 Score: 4.9 Medium (vector: CVSS:3.1/AV:P/AC:H/PR:N/UI:N/**S:C/C:H**/I:N/A:N)

- **Universal Firm Code (Firm Code > 6.000.000) with License Transfer or Borrowing**

  a) Source of the License Transfer or Borrowing is NOT a CmDongle

  If the license to be transferred or borrowed is stored in a CmActLicense or a CmCloudContainer then the threats are the same as the previous case: an attacker could extract relevant keys from a license.

  /S:C/C:H The protected product is compromised. An Attacker with a valid license might create a cryptographic hack but is not able to create a valid license.

  CVSS v3.1 Score: 4.9 Medium (CVSS:3.1/AV:P/AC:H/PR:N/UI:N/**S:C/C:H**/I:N/A:N)

b) Source of the License Transfer or Borrowing is a CmDongle

An attack would enable an attacker to create licenses that can be transferred into arbitrary CmDongles or CmActLicenses.

/S:C/C:H/I:H A scaling hack is possible which can distribute licenses that cannot be distinguished from legitimate ones.

CVSS v3.1 Score: 6.8 Medium (CVSS:3.1/AV:P/AC:H/PR:N/UI:N**/S:C/C:H/I:H**/A:N)

Remediation

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

Mitigations for affected versions

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.

Acknowledgments

We thank Infineon for reporting this vulnerability and NinjaLabs for finding it.

Disclaimer

The information in this document is subject to change without notice and should not be construed as a commitment by WIBU-SYSTEMS AG. All information that relates to the future (e.g. planned software versions and release dates) is provided without guarantee.

WIBU-SYSTEMS AG provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall WIBU-SYSTEMS AG or any of its suppliers be liable for direct, indirect, special, incidental, or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if WIBU-SYSTEMS AG or its suppliers have been advised of the possibility of such damages.

Document History

Version	Date	Description
1.0	2024-11-22	First TLP:CLEAR version