Product Security Advisory: WIBU-100031

Sharing rules

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

Vulnerability Title

Privilege Escalation in WibuKey for Windows.

Affected Products

Affected Products	Fixed Products
WibuKey < 6.71	WibuKey >= 6.71

Vulnerability Details

CVSSv3.1 Base Score(s)	8.8
CVSSv3.1 Vector(s)	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Maximal Severity	High

Vulnerabilities

An untrusted Pointer Dereference can be exploited to escalate privileges by an unprivileged user on Windows (CVE-0000-0000)

CVE-ID pending

We have requested a CVE number for this vulnerability but did not get one in time yet. This will be included once we have it.

PLEASE NOTE

The vulnerability refers **exclusively** to the legacy product **WibuKey**.
The successor product CodeMeter is NOT affected by the above-mentioned vulnerability.
Local access is needed for exploitation. The vulnerability cannot be exploited via the network.

Description

An untrusted pointer dereference in the WibuKey2_64.sys kernel driver for 64-bit Windows allows an attacker to exploit a write-what-where primitive, enabling local privilege escalation. This can be leveraged to execute arbitrary code, run an administrator shell, or gain full control over the system.

CWE: CWE-123:Write-what-where Condition

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
WibuKey < 6.71	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H	8.8

Fixed

- WibuKey >= 6.71

Remediations

Vendor fix (2025-11-12T10:00:00.000Z)

Update to Version 6.71

For products:

- WibuKey < 6.71

Mitigation (2025-11-12T10:00:00.000Z)

On systems that **use WibuKey exclusively as a network client**, the affected USB driver is not required. In this case, the WibuKey USB driver can be safely removed without any loss of functionality. This removes the vulnerable component from the system and mitigates the vulnerability. Steps:

1. **Open an elevated Command Prompt** (Run as administrator)
2. **List installed drivers**

   ```
   pnputil /enum-drivers
   ```

3. **Identify the relevant driver** In the output, locate the entry with

   ```
   Original Name : wibukeyusb.inf
   ```

   Note the **Published Name** shown for this entry (e.g., `oem7.inf`). This value will be required for the uninstall command.
   Note: The Published Name may vary between systems.
4. **Uninstall the driver**

   ```
   pnputil /delete-driver oem7.inf /uninstall
   ```

5. **Verify removal** Re-list the installed drivers:

   ```
   pnputil /enum-drivers
   ```

   The entry with

   ```
   Original Name : wibukeyusb.inf
   ```

   should no longer be present.

After completing these steps, the driver has been removed and the system is no longer vulnerable to this issue.

For products:

- WibuKey

Restart required: **machine**

Since a kernel driver is updated, we recommend a restart of the system.

Acknowledgments

- 김명규 working with Trend Micro Zero Day Initiative for discovering and reporting this vulnerability following coordinated disclosure.

WIBU-SYSTEMS AG

WIBU-SYSTEMS CERT
Zimmerstraße 5
D-76137 Karlsruhe

Namespace: https://wibu.com

cert@wibu.com

Publishing Details

Publisher	WIBU-SYSTEMS AG
Webseite	https://www.wibu.com
Security Advisories	https://www.wibu.com/support/security-advisories.html

Document Details

Document Name	WIBU-100031
Document version	1.0.0
Initial release date	2025-11-12T10:00:00.000Z
Current release date	2025-11-12T10:00:00.000Z
Language	en-US
Status	final
Also referred to	
Document category	csaf_security_advisory

Revision history

Version	Date of the revision	Summary of the revision
1.0.0	2025-11-12T10:00:00.000Z	First version

Disclaimer

Sharing rules

TLP:CLEAR

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