

Product Security Advisory: WIBU-100065

Sharing rules



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

Vulnerability Title

In the WibuKey driver, insufficient validation of user input when calculating the size of a kernel buffer could cause small amounts of data to be written outside the intended kernel buffer. This can lead to a system crash. Under unfavorable circumstances, adjacent kernel memory may be modified.

Affected Products

Affected Products

WibuKey < 6.72

Fixed Products

WibuKey >= 6.72

Vulnerability Details

Highest CVSSv3.1 Base Score	7.0
CVSSv3.1 Vector(s)	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
Highest Severity	High

Vulnerabilities

Denial of Service due to Out of Bound Write on WibuKey for Windows (CVE-2026-84854)

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 internet.

Description

WibuKey driver up to (and including) version 6.71 copies data from user space to kernel space memory. To allocate the memory in the kernel, in one instance, user input was used, which can overwrite the actual size and allocate less space than it needs for writing the data. Since the driver still writes the entire data, the final 36 Bytes are written outside of WibuKey's kernel space, thus overwriting data of an other process. In most cases, the integrity check of Windows causes a blue screen of death and thus a system crash; this would result in a CVSS-Score of CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H, resulting in 5.5 (Medium).

In theory, if a different program is running in the kernel memory with a compatible memory pattern, it could be possible to use this exploit to elevate privileges in the other application; while we stress that we failed to achieve that, we cannot rule out the possibility that this could work. As this would require a lot of overhead by forcing the memory of the other application to be adjacent in kernel memory to WibuKey, this is rated with a high attack complexity, resulting in: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H, which is 7 (High).

As we take the worst CVSS vector for each vulnerability, we stuck with the latter.

CWE: CWE-787:Out-of-bounds Write

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
WibuKey < 6.72	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	7.0

Fixed

- WibuKey >= 6.72

Acknowledgments

- 정기현(haro001)

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-100065
Document version 1.1.0
Initial release date 2026-09-30T12:00:00.000Z
Current release date 2026-09-30T12:00:00.000Z
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	2026-09-02T12:00:00.000Z	First version
1.1.0	2026-09-30T12:00:00.000Z	First public version

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. This document and parts hereof must not be reproduced or copied without written permission from WIBU-SYSTEMS AG, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose. All rights to registrations and trademarks reside with their respective owners.

Sharing rules

 TLP:CLEAR 

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