Product Security Advisory: WIBU-100057

Sharing rules

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

Vulnerability Title

User input in WibuKey is used (without proper sanitization) to compute the address of a pointer, which can be exploited to let the user point to any storage, to which Windows responds with a denial of service.

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

Denial of Service due to Improper Pointer Checks on WibuKey for 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.

Description

Improper validation of memory boundaries in WibuKey64.sys of WibuKey up to 6.70 for Windows can be exploited by an attacker by setting the pointers outside the scope of the program. This usually results in a denial of service, yet we cannot rule out the possibility of exploits that can cause Remote Code Execution and Privilege Escalation (since the driver runs with system privileges).

CWE: CWE-119:Improper Restriction of Operations within the Bounds of a Memory Buffer

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

Acknowledgments

- KEUM SUNG from Team_F1_Driver 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-100057
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/