2024-09-11
Version 1.0

Product Security Advisory WIBU-94453

Vulnerability Title

Denial of service and kernel memory corruption due to improper buffer bounds checks in WibuKey for Windows

Affected products

Product name	Affected versions	Fixed Versions
WibuKey	< 6.70 for Windows	>= 6.70

PLEASE NOTE:

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

Vulnerability CVE-2024-45181

An improper buffer bounds check in WibuKey32.sys and WibuKey64.sys allows specially crafted calls to cause arbitrary address writes, resulting in kernel memory corruption.

- CVE: CVE-2024-45181
- CVSS v3.1 base score: 8.8
- CVSS v3.1 vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
- CVSS v4.0 base score: 9.3
- CVSS v4.0 vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H
- Vulnerability type:
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2024-45182

An improper buffer bounds check in WibuKey32.sys and WibuKey64.sys allows specially crafted calls to cause an arbitrary address read, which could result in denial of service.

- CVE: CVE-2024-45182
- CVSS v3.1 base score: 6.5
- CVSS v3.1 vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H
- CVSS v4.0 base score: 8.2
- CVSS v4.0 vector: CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:H
- Vulnerability type:
  - CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Remediation

- Installation of WibuKey version 6.70 or later

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 local access is needed to exploit the vulnerabilities, it is recommended to take strict measures to control the access to the systems where the vulnerable WibuKey driver is installed.
- If a Windows server is currently used as WibuKey network license server, you can setup a WibuKey network license server on Linux or macOS instead. When using a Windows server, be sure that the local access is restricted.

General security best practices can help to protect systems from local and network attacks.

Acknowledgments

We thank Team "우리 오늘부터 0-day" and its team members: 권율(a.k.a Sechack), 강병현(a.k.a rolling), 김승찬(a.k.a zoodasa), 김종성(a.k.a nevul37), 박상준(a.k.a sangjun), 박윤진(a.k.a r136a1x27) for reporting this vulnerability following coordinated disclosure.

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	2024-09-11	First TLP:CLEAR version