**Important Information about WibuKey - Update 18 January 2019**

As announced in our last statement on December 19th, 2018, we are now coming back to you with **updated information.**

The restrictions regarding the update to the new version described in the last mail no longer apply to the release of the current update.

**Version 6.50a of WibuKey Runtime is available for download from our servers NOW:**<https://www.wibu.com/support/user/downloads-user-software.html#download-216>

The preamble: A security specialist has reported three vulnerabilities for WibuKey. These will be released on **January 24th, 2019** under the following CVE identifiers. The release date was postponed to give you enough time for an update despite the holiday season.

         CVE-2018-3989: WIBU-SYSTEMS WibuKey.sys kernel memory information disclosure vulnerability  
This CVE is a medium-severity vulnerability (CVSS rating: 4.3).  
It affects only Windows systems and allows unauthorized reading of the kernel memory information on the local system.

         CVE-2018-3990: WIBU-SYSTEMS WibuKey.sys pool corruption privilege escalation vulnerability   
This CVE is considered a critical vulnerability (CVSS rating 9.3).   
It affects only Windows systems and allows a potential unauthorized escalation of privileges on the local system.

         CVE-2018-3991: WIBU-SYSTEMS WibuKey network server management remote code execution vulnerability  
This CVE is considered a critical vulnerability (CVSS Rating 10.0).   
It affects all operating systems and potentially allows the execution of code on WibuKey network servers available in the network.  
The vulnerability affects only systems on which a WibuKey network server is running, i.e. systems that are providing licenses from a plugged-in WibuBox for use by other clients in the network.

Upon being notified, we immediately assessed the situation, analyzed the root causes, and fixed the vulnerabilities. With our own staff and in cooperation with another security service provider, we reviewed all components of WibuKey Runtime in detail and updated them to the current state of the art.

Following our assessment of the vulnerabilities, we urgently recommend an update of WibuKey Runtime to this new version on all systems not running in protected environments.

We advise you to inform your clients using WibuKey Runtime about the availability of the new version and the included fixes for the vulnerabilities and to recommend an update to this version. We are also including information for users that you can share with your clients.

***Frequently Asked Questions:***

***Q:*** How critical is the situation in practice?  
***A:*** To exploit the vulnerabilities, an attacker would have to be able to execute software on the system itself or on a system in the same network. For this to be possible, the attacker would have to have broken into the network beforehand or otherwise gained access to it. If an attacker has managed to do this, he could exploit these vulnerabilities to run code needing higher privileges on the local system or on a system running a WibuKey server on the network.

***Q:*** Do I have to install the update on all systems?  
***A:*** macOS and Linux systems that do not have any WibuKey server running are not affected by the vulnerabilities and can continue to operate the older version.

***Q:*** My systems are running in protected environments. Do I still have to install the update?  
***A:*** If you can guarantee that no attacker can access your network, you can skip the update as the vulnerabilities could not be exploited in your case.

***Q:*** Do I have to re-encrypt the protected software?  
***A:*** No. The vulnerabilities only affect components that are installed on the target system by WibuKey Runtime. In the event that you integrated WibuKey Runtime in your software’s installer, you’ll have to replace it.

***Q:*** Do the vulnerabilities allow people to circumvent the licensing and software protection?  
***A:*** No. The vulnerabilities only affect access to memory and the execution of code on the operating systems affected. This does not directly impact the licensing or protection system.

***Q:*** We are also using CodeMeter. Are these systems also affected?  
***A:*** Definitely not. The vulnerabilities apply only to WibuKey. We have also conducted an intensive check of CodeMeter Runtime in response to this situation but identified no vulnerabilities.

***Q:*** Why should I notify my users?  
***A:*** Larger companies and institutional clients often actively monitor news about security vulnerabilities. There is a certain chance that your users will themselves become aware of the situation. By notifying them proactively, you show that you accept your responsibility for the security of your users’ systems.

Please do not hesitate to contact us immediately if you have any further questions about this topic.

Please accept our apologies for any inconvenience we may have caused you!

Yours sincerely,

WIBU-SYSTEMS AG