

Karlsruhe, 19. Dezember 2018

Wichtige Information zu WibuKey

Sehr geehrte WibuKey-Anwender,

für die von Ihnen eingesetzte Software nutzt der Hersteller WibuKey zum Schutz und zur Lizenzierung. Für WibuKey sind uns von einem Sicherheitsdienstleister drei Schwachstellen gemeldet worden. Diese werden am 24.1.2019 unter den nachfolgenden Nummern veröffentlicht werden:

- CVE-2018-3989: WIBU-SYSTEMS WibuKey.sys kernel memory information disclosure vulnerability
Dieser CVE ist als mittelschwere Schwachstelle (CVSS Rating: 4,3) eingestuft worden. Die Schwachstelle betrifft nur Windows-Systeme und ermöglicht das nicht-autorisierte Auslesen von Kernel-Speicherinformationen auf dem lokalen System.
- CVE-2018-3990: WIBU-SYSTEMS WibuKey.sys pool corruption privilege escalation vulnerability
Dieser CVE ist als kritische Schwachstelle (CVSS Rating 9,3) eingestuft worden. Die Schwachstelle betrifft nur Windows-Systeme und ermöglicht eine potentielle, nicht autorisierte Rechte-Ausweitung auf dem lokalen System.
- CVE-2018-3991: WIBU-SYSTEMS WibuKey network server management remote code execution vulnerability
Dieser CVE ist als kritische Schwachstelle (CVSS Rating 10,0) eingestuft worden. Die Schwachstelle betrifft alle Betriebssysteme und ermöglicht die potentielle Ausführung von Code auf im Netzwerk erreichbaren WibuKey Netzwerk-Servern. Es sind nur die Systeme betroffen, auf denen ein WibuKey Netzwerk-Server gestartet läuft. Dies trifft also für Systeme zu, die Lizenzen einer angesteckten WibuBox im Netzwerk zur Verwendung durch andere Clients bereitstellen.

Nachdem uns diese Schwachstellen gemeldet wurden, haben wir diese umgehend bewertet, die Ursachen erforscht und behoben. Gleichzeitig haben wir sowohl im eigenen Haus als auch in Zusammenarbeit mit einem weiteren Sicherheitsdienstleister die Komponenten der WibuKey Runtime im Detail geprüft und auf den aktuellen Stand der Technik gebracht.

Ab sofort steht die Version 6.50 der WibuKey Runtime auf unseren Servern zum Download zur Verfügung:

<https://www.wibu.com/de/support/anwendersoftware/anwendersoftware.html#download-216>

Aufgrund der Einstufung der Schwachstellen empfehlen wir dringend ein Update der WibuKey Runtime auf die Version 6.50 für alle Systeme, die nicht in abgesicherten Umgebungen laufen.

WIBU-SYSTEMS AG | Rüppurrer Straße 52-54 | 76137 Karlsruhe | Deutschland

Häufig gestellte Fragen:

Frage: Wie hoch ist die Gefahr wirklich?

Antwort: Um die Schwachstellen ausnutzen zu können, muss ein Angreifer zunächst Software entweder auf dem System selbst, oder auf einem System im selben Netzwerk ausführen können. Der Angreifer muss also schon in das Netzwerk eingebrochen sein, oder sich dort Zugang verschafft haben. Wenn er dies geschafft hat, kann er die angegebenen Sicherheitslücken verwenden, um Befehle mit erhöhten Rechten lokal oder auf einem Rechner mit laufendem WibuKey-Server auszuführen.

Frage: Muss ich das Update auf allen Systemen einspielen?

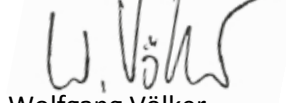
Antwort: Systeme auf macOS und Linux, die keinen WibuKey-Server gestartet haben, sind von den Sicherheitslücken nicht betroffen und können daher mit den bisherigen Versionen weiter betrieben werden.

Frage: Meine Systeme laufen in einer abgesicherten Umgebung. Muss ich trotzdem das Update einspielen?

Antwort: Wenn Sie sicherstellen können, dass Angreifer nicht in Ihrem Netzwerk Zugriff erlangen können, dann können die Schwachstellen nicht ausgenutzt werden und Sie könnten auf das Update verzichten.

Wir bitten die Unannehmlichkeiten zu entschuldigen.

Mit freundlichen Grüßen



Wolfgang Völker

Director Product Management