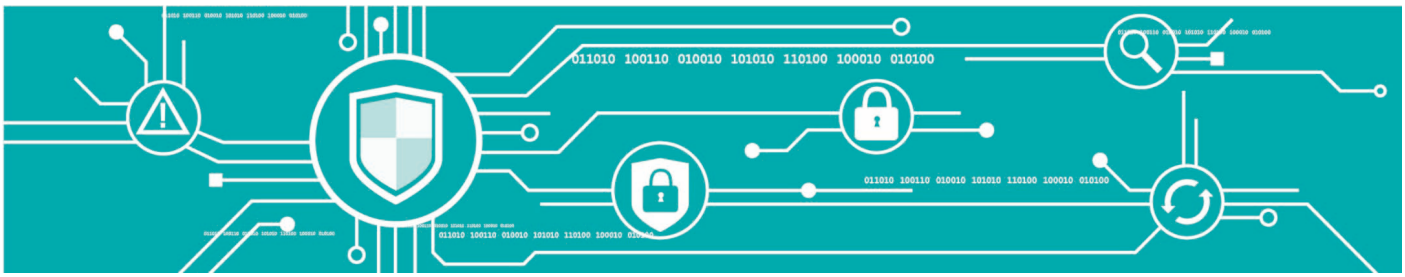

Schwachstelle in WibuKey Runtime

Mit RITOP wird auch die Software WibuKey Runtime installiert. Die installierte Version hat jedoch zwei Schwachstellen, welche die Ausführung von Remote-Code und die Offenlegung von Speicher auf der Kernelebene ermöglichen.

Um was geht es?

Es existieren mehrere Schwachstellen im WibuKey Network Server Management (Version 6.40.2402.500). Beim Produkt WibuKey Network Server Management handelt es sich um eine DRM-Lösung der Firma Wibu-Systems AG, welche von vielen namhaften Herstellern eingesetzt wird.

RITOP verwendet die Software WibuKey Runtime der Firma Wibu-Systems für die Lizenzierung.
Die Software ist auf allen RITOP Rechnern (Server und Clients) installiert und wird unabhängig von der Lizenzierungsart (Dongle oder Hardware-Fingerprint) ausgeführt.

Um die Schwachstellen auszunutzen, muss ein Angreifer ins Netzwerk eindringen oder Schadsoftware auf dem RITOP Rechner ausführen.

RIFLEX resp. **logi.CAD** setzt für die Lizenzierung auf Codemeter von Wibu-Systems (neuere Technologie) und ist von den Schwachstellen nicht betroffen.

Wie ist die Bedrohungslage auf meiner Anlage?

Die verwendete Version von WibuyKey Runtime weist zwei Schwachstellen auf, welche eine Remotecodeausführung und Speicher-Offenlegung auf Kernel-Ebene ermöglichen.

Die Serversoftware läuft standardmässig als Windows-Service und kommuniziert über Port 22347. Ein Angreifer kann ein speziell präpariertes TCP-Paket senden, um diese Schwachstelle auszunutzen und Angreifer-Code im Serverkontext auszuführen. Dieser erzeugt einen Speicherfehler (Heap-Overflow), der potentiell zu einer Remote Code Execution (RCE) genutzt werden kann.

Die zweite Schwachstelle kann nur lokal ausgenutzt werden. Ein Teil der WibuKey-Systemlösung wird durch spezielle Hardware realisiert, für die ein Treiber benötigt wird. Ein speziell präpariertes I/O-Request Packet (IRP) kann einen Speicherfehler (Buffer Overflow) im Treiber erzeugen, der zu einer Speicherkompromittierung des Kernels führt. Diese kann missbraucht werden, um beliebigen Code auszuführen und seine Rechte auf dem System zu erweitern.

Beide Bedingungen sind bei typischen RITOP Systemtopologien nicht gegeben. Solange sich die RITOP-Rechner in einem gesicherten Bereich befinden (d.h. kein Zugang durch unbefugte Personen) und die Rechner nicht ohne Firewall direkt mit dem Internet verbunden sind, wird das Gefahrenpotential und Risiko als gering eingestuft.

Wie kann ich mich dagegen schützen?

Wibu-Systems hat die WibuKey Runtime bereits auf Version 6.50b aktualisiert, welche diese Schwachstellen schliesst.

Wir haben die neue Version erfolgreich getestet und sie kann auf die bestehende Laufzeit angewendet werden.

Mit dem neusten Patch für RITOP (ab Version 2.16.1) wird auch die WibuKey Runtime auf die neue Version 6.50b aktualisiert, so dass die WibuKey Schwachstellen geschlossen werden.

Abonnenten des RITOP Patch Moduls erhalten den aktualisierten Patch automatisch (spätestens in 3 Monaten) auf ihren RITOP Rechnern installiert und müssen nichts unternehmen.

Wer kein Patch Modul Service hat, kann die WibuKey Runtime selber herunterladen und installieren https://www.wibu.com/ oder sich durch unsere Service-Hotline unterstützen lassen. Eine Anlage ohne Update-Service hat durch fehlende Windows-Updates bereits diverse Sicherheitslücken auf den Systemen.

Empfehlung

Update Service
Mit dem Update-Service übernimmt Rittmeyer das Testen und Installieren der Patches und Hotfix von Microsoft und RITOP. Besonders für das Betriebssystem wird empfohlen, in regelmässigen Abständen alle verfügbaren Sicherheitsupdates zu installieren, um bekannte Sicherheitslücken zu schliessen.

Rittmeyer AG
6341 Baar, Schweiz
T +41 41 767 10 00, F +41 41 767 10 70
security@rittmeyer.com, www.rittmeyer.com/itsecurity