Aschauer Str. 30
D-81549 München
Tel.: +49 89 62030100
Fax.: +49 89 620301069
http: //www.itWatch.de
e-Mail: info@itWatch.de

München, 09.11.2020

Sicherheitsleck CVE-2020-17022 im Windows Betriebssystem- mit itWatch bleibt trotzdem alles sicher

Wiederholt eröffnet eine Sicherheitsschwachstelle in Windows 10 Türen für Angreifer

Remote Code Execution Schwachstelle CVE-2020-17022 ermöglicht Angreifern anonym beliebigen Programmcode mit Benutzerrechten auszuführen. Diese Art der Verarbeitung von Objekten im Speicher durch die Microsoft Windows Codecs Library kann zur Ausführung von Schadcode missbraucht werden, indem das Opfersystem eine spezielle Bilddatei beispielsweise per Mail vom Angreifer empfängt.

Mit der it**W**atch **E**nterprise **S**ecurity **S**uite (itWESS) und den darin enthaltenen Modulen XRayWatch, DeviceWatch, DEvCon und ApplicationWatch können Contentfilter so gesetzt werden, dass das Verarbeiten solch schadhafter Dateien sicher verhindert wird. Diese Möglichkeit bezieht sich auf alle Formen des Zuflusses von Dateien. Zum einen kann mittels applikationsspezifischer Rechte sichergestellt werden, dass keine Anwendung (Browser, Mail etc.) solche Dateien verarbeiten kann. Zum anderen können alle Dateien solcher Art, die Peripheriegeräte / Devices an beliebigen Schnittstellen „ankommen“ sicher geblockt werden – das gilt auch für Dateien, die direkt durch das Betriebssystem eingelesen werden sollen.

Soll die Lösung ohne eine Endpoint Security Software mittels einer separierten Komponente durchgeführt werden, so bietet itWatch mit itWash, einer Datenschleuse mit Datenwäsche, eine geeignete Lösung. itWash ermöglicht es durch Prüfung und Konvertierung in sichere Dateiformate sogar, die betroffenen Dateien so zu modifizieren (Datenwäsche), dass der Inhalt der Datei befreit von den problematischen Elementen weiterverarbeitet werden kann.

Nähere Informationen finden Sie unter www.itWatch.de