Warnung vor Sicherheitsrisiko am 05.07.: Systeme neu starten, Druckerwarteschlange deaktivieren

(Please scroll down for English version)

Eine kritische Sicherheitslücke in Microsoft Windows Betriebssystemen erfordert eine schnelle Reaktion des Universitätsrechenzentrums. Dabei wird dringend um Ihre Mithilfe gebeten. Starten Sie alle Windows-Geräte, welche zur Universität Jena gehören, unverzüglich neu. Nur so können die sicherheitsrelevanten Richtlinien auf Ihren Geräten greifen.

Mit dieser Gegenmaßnahme sind einige Unannehmlichkeiten bzgl. des Druckens verbunden.

Das Ausdrucken von Dokumenten wird nur noch an folgenden Druckerarten möglich sein:

- lokal am Rechner angeschlossene Drucker
- Netzwerkdrucker, welche über die Druckserver des Universitätsrechenzentrums bereitgestellt werden
- thoska-Drucker auf dem Campus

Das Ausdrucken wird nicht mehr über Druckerfreigaben von Windows-Rechnern funktionieren.

Betreiber von Windows-Servern werden zum unverzüglichen Handeln aufgefordert. Wie Sie ihr privates Gerät vorübergehend schützen können, bis ein Patch von Microsoft veröffentlicht ist, lesen Sie hier:

<https://www.heise.de/news/Jetzt-handeln-Angreifer-nutzen-die-Drucker-Luecke-in-Windows-bereits-aus-6127265.html>

Vielen Dank für Ihre Mithilfe.

—

A critical vulnerability in Microsoft Windows operating systems requires a rapid response from the university data center. We urgently ask for your help. Please restart all Windows devices of the University Jena immediately. This is the only way to implement the security-relevant guidelines on your devices.

With this countermeasure, there is some inconvenience related to printing.

It will only be possible to print documents on the following types of printer:

- printers connected locally to computers
- network printers, which are available via the print server of the university computer center
- the thoska printers on campus

Printing will no longer work via printer shares from Windows computers.

Windows server operators are requested to act immediately. For further technical information and how to protect your personal device please visit:

<https://blog.truesec.com/2021/06/30/fix-for-printnightmare-cve-2021-1675-exploit-to-keep-your-print-servers-running-while-a-patch-is-not-available/>

Thank you for your help.