

Improving our compliance IQ

Trending topics: 28th Sep 2020

Major Instagram App Bug Could've Given Hackers Remote Access to Your Phone



“Ever wonder how hackers can hack your smartphone remotely?”

Check Point researchers disclosed details about a critical vulnerability in Instagram's Android app that could have allowed remote attackers to take control over a targeted device just by sending victims a specially crafted image.

What's more worrisome is that the flaw not only lets attackers perform actions on behalf of the user within the Instagram app—including spying on victim's private messages and even deleting or posting photos from their accounts—but also execute arbitrary code on the device.

According to an advisory published by Facebook, the heap overflow security issue (tracked as CVE-2020-1895, CVSS score: 7.8) impacts all versions of the Instagram app prior to 128.0.0.26.128, which was released on February 10 earlier this year.” ...

Sep24, 2020

Read more... [The Hacker News](#)

Tyler Technologies Suffers Apparent Ransomware Attack



“Plano, Texas-based Tyler provides end-to-end information management solutions to more than 15,000 local government offices in all 50 states, Canada, the Caribbean, and Australia.

Tyler Technologies – one of the largest solution providers to state and local government in the U.S. – was hit in an apparent ransomware attack, according to KrebsOnSecurity.

Cybersecurity reporter Brian Krebs said the company copped to an intrusion to its system, but told him it was limited to internal company systems and had no impact on its customers.

Sen 23, 2020

Read more... [CRN](#)

A Patient Dies After Ransomware Attack Paralyzes German Hospital Systems



“German authorities last week disclosed that a ransomware attack on the University Hospital of Düsseldorf (UKD) caused a failure of IT systems, resulting in the death of a woman who had to be sent to another hospital that was 20 miles away.

The incident marks the first recorded casualty as a consequence of cyberattacks on critical healthcare facilities, which has ramped up in recent months.

The attack, which exploited a Citrix ADC CVE-2019-19781 vulnerability to cripple the hospital systems on September 10, is said to have been "misdirected" in that it was originally intended for Heinrich Heine University, according to an extortion note left by the perpetrators.”

Sept. 21, 2020

Read more... [The Hacker News](#)