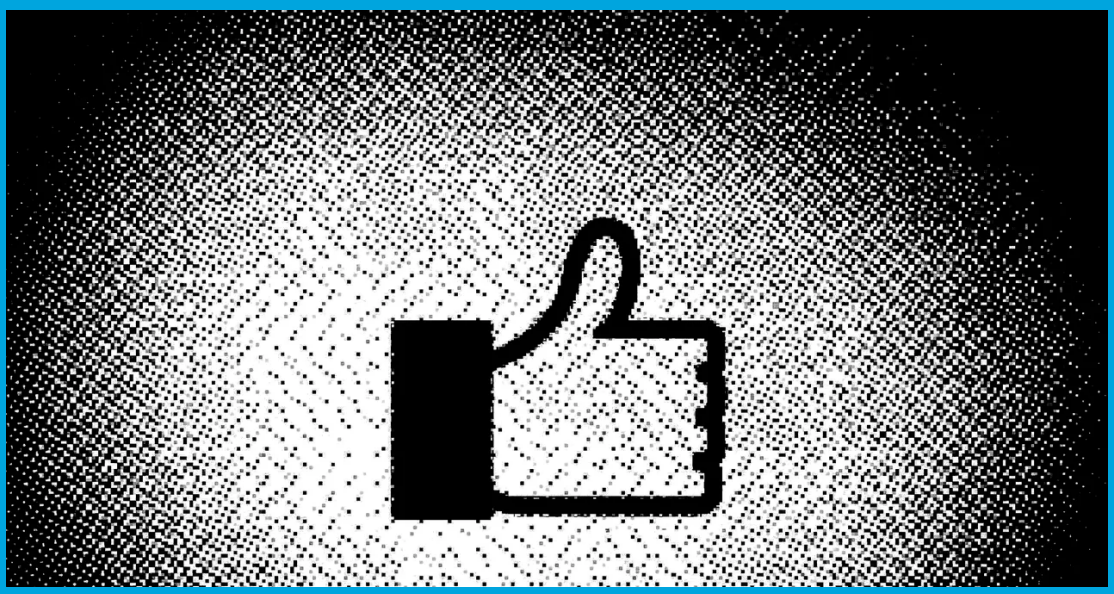
kindred

Security Newsletter

15 Aug 2022

Subscribe to this newsletter

Will Europe Force a Facebook Blackout?



Facebook faces trouble in Europe—and Meta wants you to know about it. Every three months since June 2018, the company has used its financial results to warn that it could be forced to stop running Facebook and Instagram across the continent—potentially pulling its apps from millions of people and thousands of businesses—if it can't send data between the EU and the US.

Data regulators are on the verge of making a historic ruling in a years-long case, and they are expected to say Facebook's data transfers across the Atlantic should be blocked. For years, Meta has fought against European privacy activists over how data is sent to the US, with courts ruling multiple times that European data isn't properly protected and can potentially be snooped on by the NSA and other US intelligence agencies.

While the case focuses on Meta, it has widespread ramifications, potentially impacting thousands of businesses across Europe that rely upon the services of Google, Amazon, Microsoft, and more.

Read More on Wired

A New Jailbreak for John Deere Tractors Rides the Right-to-Repair Wave

Farmers around the world have turned to tractor hacking so they can bypass the digital locks that manufacturers impose on their vehicles. Like insulin pump “looping” and iPhone jailbreaking, this allows farmers to modify and repair the expensive equipment that’s vital to their work, the way they could with analog tractors. At the DefCon security conference in Las Vegas on Saturday, the hacker known as Sick Codes is presenting a new jailbreak for John Deere & Co. tractors that allows him to take control of multiple models through their touchscreens.

The finding underscores the security implications of the right-to-repair movement. The tractor exploitation that Sick Codes uncovered isn't a remote attack, but the vulnerabilities involved represent fundamental insecurities in the devices that could be exploited by malicious actors or potentially chained with other vulnerabilities. Securing the agriculture industry and food supply chain is crucial, as incidents like the 2021 JBS Meat ransomware attack have shown. At the same time, though, vulnerabilities like the ones that Sick Codes found help farmers do what they need to do with their own equipment.

Read More on Wired

More #News

- Google fined $60 million over Android location data collection
- Sounding the Alarm on Emergency Alert System Flaws
- US govt will pay you $10 million for info on Conti ransomware members
- It Might Be Our Data, But It's Not Our Breach
- Google now blocks Workspace account hijacking attempts automatically
- The Security Pros and Cons of Using Email Aliases
- How hackers are stealing credit cards from classifieds sites
- Can you stop your open-source project from being used for evil?
- Facebook Testing Default End-to-End Encryption and Encrypted Backups in Messenger
- Vulnerabilities Allowed Researchers to Remotely Lock and Unlock Doors

#Breach Log

- Twilio: 125 customers affected by data breach, no passwords stolen
- Zimbra auth bypass bug exploited to breach over 1,000 servers
- 7-Eleven Denmark confirms ransomware attack behind store closures
- Automotive supplier breached by 3 ransomware gangs in 2 weeks
- Cisco hacked by Yanluowang ransomware gang, 2.8GB allegedly stolen
- Twitter Exposes Personal Information for 5.4 Million Accounts

#Patch Time!

- Cisco fixes bug allowing RSA private key theft on ASA, FTD devices
- Microsoft Patch Tuesday, August 2022 Edition
- Microsoft patches Windows DogWalk zero-day exploited in attacks
- VMware warns of public exploit for critical auth bypass vulnerability

#Tech and #Tools

- Microsoft blocks UEFI bootloaders enabling Windows Secure Boot bypass
- Researching Xiaomi's TEE to get to Chinese money
- The Millennium Problem
- Browser-Powered Desync Attacks: A New Frontier in HTTP Request Smuggling

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering more than 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 2,000 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

You can access the previous newsletters at https://news.infosecgur.us