TechTips Newsletter

tech hero

Insider Tips To Make Your Business Run Faster, Easier And More Profitably

DATABASE MISCONFIGURATION EXPOSES 100 MILLION ANDROID USERS TO DATA LEAK

Researchers at Check Point released a report showing how roughly 100 million Android users have been exposed to a data leak. The cause is a misconfiguration of real-time databases tied to numerous third-party Android OS applications (13 in total). The specific issue has to do with app developers not being meticulous when integrating their products with third-party cloud services. The result is chat logs, passwords, location data, and numerous other sensitive data logs exposed to threat actors.

Check Point's report explains the configuration issue behind this Android data leak on a more technical level in the following excerpt:

Continued on next page...

June 2021

This monthly publication provided courtesy of Adam Cambreleng, Inside Account Manager here at Tech Hero

Our Mission

To build a community of successful minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

"Real-time databases allow application developers to store data on the cloud, making sure it is synchronized in real-time to every connected client. This service solves one of the most encountered problems in application development, while making sure that the database is supported for all client platforms. However, what happens if the developers behind the application do not configure their real-time database with a simple and basic feature like authentication?

This misconfiguration of real-time databases is not new, and continues to be widely common, affecting millions of users. All CPR researchers had to do was attempt to access the data. There was nothing in place to stop the unauthorized access from happening."

What this situation shows is two major issues — two that are in some ways connected. The first is that application developers often ask for incredibly sensitive data to perform tasks that really do not require it. One example of the applications was a horoscope service that asked for a large amount of personal data. Why on earth do you need to give your extensive background to an automated program for an astrology reading?

Secondly, this shows that privacy and data protections cannot be expected when using any application. Ultimately, users need to be defensive of every single thing they use on their devices. If an app for some frivolous purpose, or even something more serious, asks for a large amount of personal information, perhaps consider whether you truly need to take the risk.

Data leaks are happening at an alarmingly accelerating rate, and ultimately it is up to the individual how much they wish to risk in this technological hellscape.

—Derek Kortepeter, TechGenix

tech hero

Cloud Portal

Did you know about our new Cloud Portal? This new tool will allow you to open tickets directly with us here at Tech Hero at the click of a button!

To try it out, just go down to your system tray and look for the small blue IT icon. After you've double clicked on it you will need to sign in (You will only need to do this once!)

Once you are in you can click around explore the software.

If you have any questions, feel free to reach out to us at the number below!

(800) 900-TECH x2

vmware PARTNER

PROFESSIONAL SOLUTION PROVIDER

Free Consultation to review your VMware Licensing!

Contact your Tech Hero sales representative to schedule a FREE review of your VMware licensing.

Find out ways to save money, ways to receive free upgrades, and a better understanding on the VMware license models.

tech hero

1-(800) 900-TECH (option 2)

Sales@TechHero.com

CARNIVAL CRUISE LINE HIT BY CYBERATTACK, PERSONAL DATA BREACHED

According to an internal letter sent by Carnival Corp., the parent company of Carnival Cruise Line, the major provider of cruises has experienced a cyberattack. The letter was sent to customers of Carnival and was first obtained by Bleeping Computer's Sergiu Gatlan. According to the letter, Carnival came under attack on March 19 via an unnamed malicious actor. The letter initially states that only email accounts were accessed, but Carnival's senior vice president and chief communications officer Roger Frizzell updated Bleeping Computer by stating that there was also a breach in IT systems.

The letter to affected Carnival customers states that "The impacted information includes data routinely collected during the guest experience and travel booking process or through the course of employment or providing services to the Company, including COVID or other safety testing." The information belongs primarily to customers, but Carnival staff are also reportedly affected by this breach.

Continued on next page...

Carnival is offering free credit monitoring to customers for 18 months in the aftermath of the cyberattack. Much of the data stolen can, and most likely will, find its way to underground forums on the Dark Web. Cybercriminals will then use this data to commit various instances of fraud and malicious social engineering campaigns. Anyone possibly affected by this should monitor their financial accounts very carefully and report any suspicious activity.

As the world is slowly starting to re-embrace travel in this pandemic, cruise lines, in particular, are looking to hit the ground running. Carnival could not have had this occur at a worse time, especially considering that this is just the latest in a line of major cyberattacks on the company. Starting in 2020, Carnival experienced ransomware attacks and other cyberattacks that have been bad PR for the company. After a while, people stop trusting an organization that continuously cannot defend against cybercriminals.

For this reason, Carnival should look to audit every system and plug every hole in its defenses. Whatever they have been doing has simply not been enough.

—*Derek Kortepeter for Techgenix*

Client Spotlight

THE FLORIDA BAR FOUNDATION

The Florida Bar Foundation provides greater access to justice in Florida through strategic grantmaking and investments in assessment, training, technology and technical assistance to help grantees build capacity and operate efficiently and effectively. Our board, among other things, allocates several grant funds annually, including three Florida Supreme Court approved uses of funds from Florida's Interest on Trust Accounts (IOTA) program.

IKEA FRANCE PUNISHED FOR SPYING ON ITS EMPLOYEES

Swedish furniture giant IKEA has been hit with a fine of €1 million (about $1.2 million). The fine comes after an investigation into IKEA's French retail division that resulted in a trial for spying primarily on employees. According to AFP, French courts in Versailles ruled that IKEA France engaged in a spying scheme that affected numerous employees. Additionally, Jean-Louis Baillot, head of IKEA France at the time of the crimes, was given an 18-month suspended prison sentence and was ordered to pay €50,000 in restitution.

The courts focused on a series of IKEA spying incidents that occurred between the years 2009 and 2012. Though prosecutors assert that the system used to surveil existed longer than this, the most damning evidence comes from this time frame. French media reported in 2012 that, in AFP's words, "IKEA's management had obtained private personal data on employees, including people active in labor unions or works councils." Such data ranged from private purchases made by employees to their political affiliations or activities related to these political affiliations. The surveillance network was elaborate and sought to dig into countless details of employees' private lives.

Continued on next page...

Baillot asserted his innocence throughout the trial and subsequent ruling, stating that he was considering an appeal. IKEA France issued the following statement following the conclusion of the case:

"Ikea takes the protection of co-worker and customer data very seriously... IKEARetail France has strongly condemned the practices, apologized and implemented a major action plan to prevent this from happening again... We will now review the court's decision in detail and consider if and where any additional measures are necessary."

Though IKEA's reputation has taken a hit from this case, many affected by the spying do not believe the ruling is strong enough. Alexis Perrin, a lawyer for IKEA union members in Lyon, stated as much by saying, "These amounts are not enough to force IKEA or other companies to change their behavior." In all, the 120 plaintiffs in the case are expected to receive €1,000 to €10,000 each. —*Derek Kortepeter for Techgenix*