

Mobile App Breaches of 2022

Organizations that suffer mobile application security and privacy breaches know all too well the damage they can incur — tarnished brand reputation, loss of customer trust, depressed shareholder value and exposure to regulatory compliance fines and legal settlements.

Today, companies need to not only manage the risk in the mobile apps they build, but also guard against supply-chain vulnerabilities found in software libraries and third-party components used in their mobile code. The secure mobile app development mistakes continue to mount.

This year alone, Check Point Research discovered that 2,113 mobile apps using the Firebase database exposed data.¹ More than 2,100 mobile apps leaked Twitter API keys, potentially allowing account takeover.² And thousands of apps were found to contain hardcoded Amazon Web Services (AWS) access tokens that could be used to access corporate data from the cloud.³ Worse, the NowSecure MobileRiskTracker finds that some 85% of mobile apps in the Apple App Store and Google Play contain security and privacy vulnerabilities.

What follows are some of the most notable or impactful mobile AppSec issues of 2022.



January

My2022



The **My2022** mandatory Olympic Games mobile app for attendees failed to validate SSL certificates and had an encryption flaw that exposed large volumes of sensitive health and travel information.⁴

March



Kurbo by WW

The Federal Trade Commission fined WW International \$1.5 million because its **Kurbo by WW** mobile app illegally collected kids' sensitive health data in violation of the Children's Online Privacy Protection Act (COPPA).⁵

June

Tim Hortons



A Canadian government investigation concluded the **Tim Hortons** mobile app unnecessarily collected extensive personal information that constituted an invasion of users' privacy.⁶

August



TikTok

A high-severity vulnerability in the **TikTok** Android app downloaded by more than a billion users around the globe could enable attackers to compromise accounts with a single click.⁷

December

MyHyundai & MyGenesis



Vulnerabilities in the **MyHyundai** and **MyGenesis** mobile apps allowed security researchers to remotely unlock, start, stop and lock the vehicles.⁸

⁴Citizen Lab, "Cross-Country Exposure: Analysis of the MY2022 Olympics App," Jan. 18, 2022

⁵CBS News, "Weight Watchers diet app collected data on kids as young as 8, FTC says," March 4, 2022

⁶Bloomberg, "Tim Horton App Tracked People Illegally, Canada Watchdogs Say," June 1, 2022

⁷Microsoft, "Vulnerability in TikTok Android app could lead to one click account hijacking," Aug. 31, 2022

⁸BleepingComputer, "Hyundai app bugs allowed hackers to remotely unlock, start cars," Dec. 1, 2022



Don't Fall Victim to a Mobile Cyberattack



Ensure your organization doesn't release or use mobile apps with security and privacy vulnerabilities. Deploy integrated mobile application security testing in the DevSecOps pipeline and perform mobile app vetting for supply-chain risk management with NowSecure Platform. Additionally, tap NowSecure Mobile Pen Testing as a Service (PTaaS) to scale security more efficiently. Reach out for a free demo.