LILY HAY NEWMAN SECURITY 03.04.2021 10:00 AM

Thousands of Android and iOS Apps Leak Data From the Cloud

It's the digital equivalent of leaving your windows or doors open when you leave the house—and in some cases, leaving them open all the time.

PHOTOGRAPH: ÁLEX CÁMARA/GETTY IMAGES

FOR YEARS, SIMPLE setup errors have been a major source of exposure when companies keep data in the cloud. Instead of carefully restricting who can access the information stored in their cloud infrastructure, organizations too often misconfigure their defenses. It's the digital equivalent of leaving the windows or doors open at your house before going on a long vacation. That leaky data problem applies to more than just the web services that typically grab headlines. Mobile security firm Zimperium has found that these exposures pose a major problem for iOS and Android apps as well.

Zimperium ran automated analysis on more than 1.3 million Android and iOS apps to detect common cloud misconfigurations that exposed data. The researchers found almost 84,000 Android apps and nearly 47,000 iOS apps using public cloud services—like Amazon Web Services, Google Cloud, or Microsoft Azure—in their backend as opposed to running their own servers. Of those, the researchers found misconfigurations in 14 percent of those totals—11,877 Android apps and 6,608 iOS apps—exposing users' personal information, passwords, and even medical information.

“It's a disturbing trend,” says Shridhar Mittal, Zimperium's CEO. “A lot of these apps have cloud storage that was not configured properly by the developer or whoever set things up and, because of that, data is visible to just about anyone. And most of us have some of these apps right now.”

The researchers reached out to a handful of the app makers they found with cloud exposures, but they say the response was minimal and many apps still have exposed data. This is why Zimperium isn't naming affected apps in their report. Additionally, the researchers can't notify tens of thousands of developers. Mittal says, though, that the services they looked at run the gamut from apps with a few thousand users to those with a few million. One of the apps in question is a mobile wallet from a Fortune 500 company that's exposing some user session information and financial data. Another is a transportation app from a large city that's exposing payment data. The researchers also found medical apps with test results and even users' profile images out in the open.

Given that Zimperium found nearly 20,000 apps with cloud misconfigurations, the company didn't attempt to individually assess whether attackers have already discovered and abused any of the exposures. But these open doors and windows would be easy for bad actors to find using the same publicly available information that Zimperium used in its research. Hacking groups already do this type of scanning to find cloud misconfigurations in web services. And Mittal says that, in addition to sensitive user data, the researchers also found network credentials, system configuration files, and server architecture keys in some of the exposed app storage that attackers could potentially use to gain deeper access to an organization's digital systems.

On top of all of that, the researchers found that some of the misconfigurations would allow bad actors to change or overwrite data, creating additional potential for fraud and disruption.

Though major cloud providers like AWS have made an effort to proactively detect possible misconfigurations and warn customers about them, it ultimately comes down to developers and IT administrators checking to confirm that things are set up as intended.

“It absolutely makes sense that misconfiguration could be a widespread issue,” says Will Strafach, a longtime iOS security researcher and creator of the Guardian Firewall app. "I've seen AWS buckets with bad permissions, and I've also seen multiple VPN nodes exposing data. I've seen a lot of apps from companies who should know better that have horrible security issues.”

Zimperium is one of three mobile security firms that participates in Google's App Defense Alliance initiative, conducting automated app scanning for the company's Google Play store. Zimperium's Mittal says the company uses the same tools for the App Defense Alliance work that the researchers used in their investigation of cloud misconfigurations. But when scanning for the Alliance, Zimperium looks for potentially malicious functionality rather than accidental exposures.

Mittal hopes that raising awareness about mobile cloud misconfigurations will motivate developers to take a closer look at their infrastructure and flip a few switches to lock things down. But given how difficult it can be to reach the right person within an organization—and

how common it is for companies to outsource the development of their own apps—it will likely take time to solve the problem.

“For users, their personally identifying information could be exposed, medical information, test results, phone numbers, even passwords to certain accounts," Mittal says. "And for enterprises this creates risk, too. Attackers could gather information that helps them hack in deeper.”

There are a lot of security protections that are difficult to implement and that organizations may even intentionally avoid, like patching always-on systems or replacing vulnerable hardware. When it comes to dealing with cloud misconfigurations, though, most apps will just need to check some boxes to significantly improve their data privacy and security.

More Great WIRED Stories

- 📨 The latest on tech, science, and more: Get our newsletters!
- Sex tapes, hush money, and Hollywood’s economy of secrets
- Twinkling black holes reveal an invisible cloud in our galaxy
- The woman bulldozing video games’ toughest DRM
- OOO: Help! Everyone is judging my messy bedroom
- The best emergency gear to keep at home
- 🎮 WIRED Games: Get the latest tips, reviews, and more
- ▫▫▫ Want the best tools to get healthy? Check out our Gear team’s picks for the best fitness trackers, running gear (including shoes and socks), and best headphones

---

Lily Hay Newman is a senior writer at WIRED focused on information security, digital privacy, and hacking. She previously worked as a technology reporter at Slate magazine and was the staff writer for