HighTech

NowSecure®

High-Tech Apps Expose Data

Security and privacy vulnerabilities in popular business software could spill corporate secrets.

With remote work here to stay, usage of enterprise business-to-business (B2B) mobile apps continues to grow. These high-tech tools help organizations automate operations, enhance efficiencies, grow sales and improve customer service.

In the quest to quickly develop new capabilities to improve the user experience and attract customers, some mobile app developers unknowingly build apps that contain security and privacy bugs. But overlooking mobile AppSec in the development process can cause a data breach that imperils the enterprise.

Business Apps Enhance Efficiency

People spend many hours using mobile apps to meet and communicate with colleagues and access information.

~1.5 billion
Business software mobile app downloads in 2022[1]

5 hours, 2 minutes
Average daily time spent in mobile apps per user[2]

> 267,000

Number of downloads in a single day prompted by surging interest in Chatbot[3]

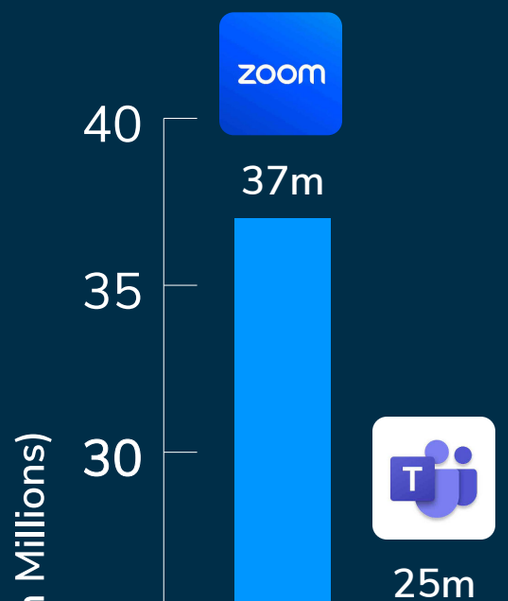
[1]Data.ai, "State of Mobile 2023," January 2023

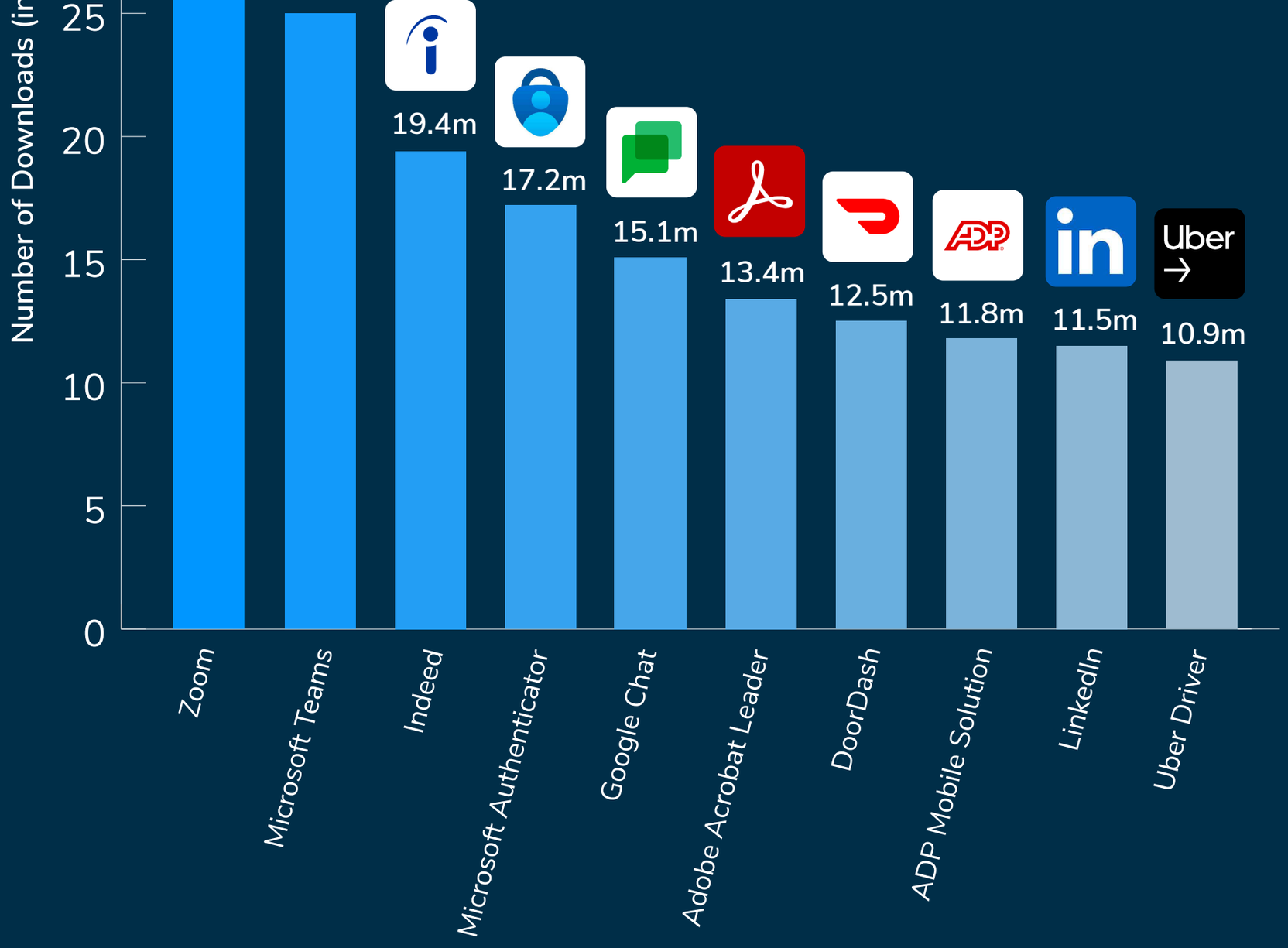
[2]Data.ai, "Welcome to the Half-Trillion Dollar App Market," Jan. 18, 2023

[3]Business Insider, "Even at its weirdest, unhinged moments, Bing's chatbot is making Microsoft relevant again," March 1, 2023

Most Downloaded Business Apps

Remote work continued to drive video conferencing while job hunting and networking spurred use of Indeed and LinkedIn.[4]

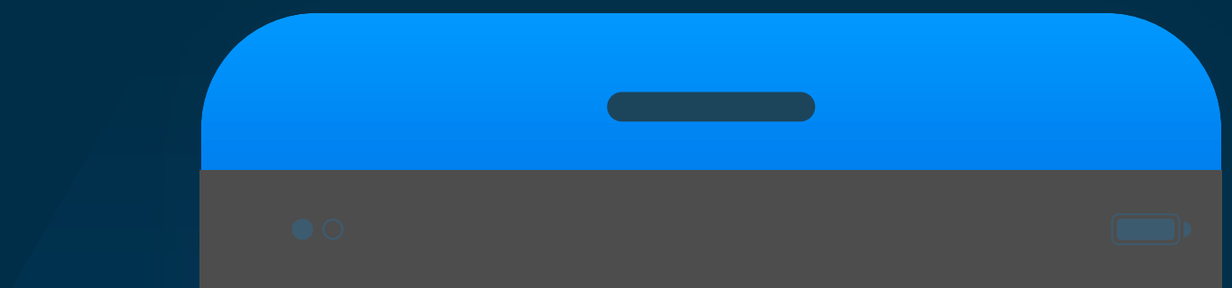




[4]Finbold, "Zoom is the most downloaded business app in the U.S. followed by Microsoft Teams," Feb. 21, 2023

Mobile Breaches Damage Companies

Poor security and privacy practices undermine user trust, erode brand reputation, incur regulatory fines and invite lawsuits.



A threat actor exploited an API vulnerability in the Twitter Android client to expose more than 5.4 million user records before the vulnerability was fixed.[5]

Researchers discovered a zero-day vulnerability in Apple iMessage enabled spyware to seize control of iPhones, iPads, Apple Watches and MacBook computers.[6]

Preinstalled mobile app on Samsung devices contained security flaws that left them open to data theft.[7]

A bug in the Android version of Slack exposed user credentials in clear text.[8]

[5]Bleeping Computer, "Twitter confirms zero-day used to expose data of 5.4 million accounts," Aug. 5, 2022
[6]NBC News, "Update your iPhone: Spyware company using 'terrifying' hack, researchers say," Sept. 13, 2021
[7]TechCrunch, "Security flaws found in Samsung's stock mobile apps," June 10, 2021
[8]The Verge, "PSA: if you use Slack on Android, you might want to update your password," Feb. 11, 2021

Apps Suffer from Insufficient Security

NowSecure MobileRiskTracker benchmark testing reveals hundreds of high-tech apps have security and privacy vulnerabilities.[8]

74
Average risk score out of 100 equating to a 'C'

99%
of high-tech apps have at least 1 or more letter grade

86%
of high-tech apps use dangerous permissions

security risks

42%
of high-tech apps use weak cryptography

[8]NowSecure, MobileRiskTracker, March 2, 2023

Improve Enterprise App Security

High-tech and B2B software builders can take the following steps to reduce risk in their mobile apps:

- Embrace proven industry standards of OWASP MAS
- Upskill developers on secure coding practices
- Integrate continuous mobile application security into the dev pipeline
- Conduct pen testing on sensitive mobile apps or major new releases
- Monitor mobile apps in production for supply-chain vulnerabilities

Get a demo to see how NowSecure Platform helps companies safeguard their mobile apps and explore NowSecure Mobile Pen Testing as a Service (PTaaS).

© 2023 NowSecure. All Rights Reserved.