Software Supply-Chain Attacks Unfold Across the Globe

Supply-chain risk management can help protect organizations from security vulnerabilities in third-party code and third-party mobile apps.

NowSecure™
MOBILE APP TRENDS

Escalating software supply-chain attacks pose a serious threat to the public sector and businesses. Adversaries exploit vulnerabilities in third-party code to compromise a supplier to the vast digital ecosystem downstream. The ripple effect causes widespread disruption, financial loss and reputational damage and even endangers national security.

Consider the enormous impact the SolarWinds software supply-chain attack had on the private sector and U.S. federal, state and local governments then think of the thousands of web and mobile applications that are under attack. Notable mobile apps that suffered data breaches in 2021 include Apple iMessage, Klarna, ParkMobile, Samsung SecureFolder and Slack.

As developers increasingly rely on code libraries and open-source components to quickly build mobile apps and enterprises deploy more third-party apps, the complexity of the software supply chain grows. The Apple App Store™ and Google Play™ house some 6 million apps[1] and don't include countless other custom mobile apps companies develop in house or obtain from vendors and consultants. That makes for a massive threat landscape in which a single weak link can lead to an attacker infiltrating systems around the globe.[2]

Breaches Unleash Extensive Damage

Skyrocketing reports of software supply-chain security incidents demonstrate the struggle to manage software supply-chain risk. The European Union Agency for Cybersecurity (ENISA) estimated a 4x increase in supply-chain attacks in 2021.[3] Sonatype research revealed a 650% increase in next-generation cyberattacks against open-source tools over a one-year period.[4] And Forrester forecasts that 60% of cybersecurity incidents in 2022 will result from issues with third parties.[5]

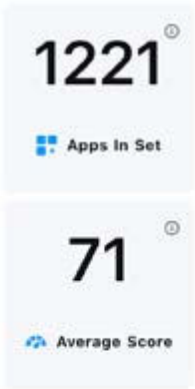
of security issues will be caused by third parties[5]

Software supply-chain attacks have far-reaching impacts and organizations face considerable challenges and expense to remediate them. A CloudBees survey revealed 64% of C-suite executives said it would take more than four days to mitigate a software supply-chain incident.[6] But some may not even know when their businesses are attacked. Another report found more than one-third of leaders have no way of knowing if or when a cybersecurity issue with a third party arises.[7]

Complex layers of software interdependencies makes supply-chain attacks incredibly expensive — some 10x more costly than traditional breaches. RiskRecon estimates financial losses directly tied to software supply-chain attacks amount to an astounding $7.4 billion.[8]

Security Risks Lurk Within App Stores

The NowSecure Mobile Risk Tracker real-time benchmarking tool continuously monitors the top 5,200 mobile apps across key industries to provide visibility into security and privacy issues in the mobile app supply chain.



NowSecure™
MOBILE APP TRENDS

Organizations must rapidly improve the security and integrity of the software supply chain.

U.S. Government Strengthens Cyberdefenses

Alarmed by growing risk to the software supply chain, the U.S. government has acted to fight the threat. In 2021, the White House issued an Executive Order mandating cybersecurity requirements for federal agencies, systems integrators, vendors and contractors.[9] "The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy," the EO states.[10] "The federal government must take action to rapidly improve the security and integrity of the software supply chain, with a priority on addressing critical software."

In addition, the Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute of Standards and Technology (NIST) recently offered guidance to the private sector about mitigating software supply-chain risk.[11] And as part of the cybersecurity EO directive, NIST has defined critical software[12] and is updating a set of best practices for secure software delivery[13] and software labeling.[14]

Safeguard the Mobile App Supply Chain

Security and DevSecOps leaders should adopt cyber supply chain risk management strategies to safeguard their mobile applications from attack. Here are a few initial steps to take.

10x

Cost of software supply-chain breaches compared to traditional breaches[15]

- Create and maintain a Software Bill of Materials (SBOM) to uncover risks hiding in open-source and third-party components that your development team uses to build mobile apps.
- Ask your software vendors to provide SBOMs and confirmation that their mobile apps are safe to use.
- Gain visibility into your existing mobile app portfolio by conducting an inventory and vetting for security, privacy and compliance issues.
- Perform continuous monitoring to stay on top of new vulnerabilities or dependency changes that introduce security, privacy or compliance risks.

About NowSecure

NowSecure offers a comprehensive suite of automated mobile app security and privacy testing solutions, penetration testing and training services to reduce risk. Trusted by many of the world's most demanding organizations, NowSecure protects millions of app users across banking, insurance, high tech, retail, healthcare, government, IoT and others. As the recognized expert in mobile app security, NowSecure was recently named a mobile security testing leader by IDC, a DevSecOps transformational leader by Gartner, a Deloitte Technology Fast 500 winner and a TAG Distinguished Vendor.

Visit www.nowsecure.com to learn about strategies for reducing risk from the mobile app supply chain and get a free SBOM report.

SOURCES

1 Business of Apps, "App Store Data 2021," November 2021

2 NowSecure, "Beware of Mobile App Supply-Chain Attacks," February 2021

3 European Union Agency for Cybersecurity, "Threat Landscape for Supply Chain Attacks," July 2021

4 Sonatype, "2021 State of the Software Supply Chain," September 2021

5 Forrester, "Predictions 2022: Continued Uncertainty Focuses Attention on Securing Relationships," October 2021

6 CloudBees, "Global C-Suite Security Survey," September 2021

7 BlueVoyant, "Managing Cyber Risk Across the Extended Vendor Ecosystem," October 2021

8 RiskRecon, "Ripples Across the Risk Surface," 2021

9 The White House, "Executive Order on Improving the Nation's Cybersecurity," May 2021

10 NowSecure, "Cybersecurity Executive Order Impacts Mobile Apps," August 2021

11 Cybersecurity and Infrastructure Security Agency, "Defending Against Software Supply Chain Attacks," April 2021

12 National Institute of Standards and Technology, "Definition of Critical Software Under Executive Order (EO) 14028," October 2021

13 The White House, "FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity," August 2021

14 CSO, "NIST gears up for software security and IoT labeling pilot programs," Dec. 13, 2021

15 RiskRecon, "Ripples Across the Risk Surface," 2021