



Pinduoduo App



Overview

Pinduoduo, a large Chinese online retailer, recently had their app removed from both the Google Play Store and iOS App Store because of malicious activity in their app. Researchers have <u>reported</u> that certain versions of this app contain code that can exploit the operating system of devices running the app and could prevent the user from removing the app from the device, installing additional malware in the background, removing other legitimate applications, and spying on the user.

Lookout Coverage and Recommendation for Admins

Lookout already has a coverage in place for this app. Any new or existing download of a malicious version of the app will be reported. Additionally, please set the Out of date ASPL policy to have a minimum of March 2023. They can then choose whether to alert the user that the device is out of compliance or block access to enterprise resources until ASPL is updated. We strongly suggest users to keep their devices on auto update for security fixes as and when they become available. Furthermore, we advise the admins to denylist the application for both Android and iOS if they find the app in their fleet.

Lookout Analysis

Lookout Researchers have confirmed that the alleged malicious functionality exists in versions that exist outside of Google Play as well. We have no indication at this time that Pinduoduo's iOS app is affected. Our detailed analysis of the exploits used reveals that one of them relied on CVE-2023-20963, a vulnerability affecting essentially all current Android devices and fixed only in the March 2023 ASPL.

Malicious versions of Pinduoduo were signed with the same signing key as the Pinduoduo app that was distributed via Google Play until it was removed from the store. This proves that the creators of the malicious app have access to the same signing keys as the creators of the legitimate app that was available from Play. Given that a malicious actor had the ability to produce legitimately-signed apps we advise our customers to denylist the Pinduoduo app (com.xunmeng.pinduoduo) for their users, if they find it in their fleet.

Lookout Vulnerability and Patch Management

Lookout Vulnerability and Patch Management enables you to know every version of an operating system and mobile app in your organization. We provide visibility into device risk whether it is company- or employee-owned, as well as managed or unmanaged.

Click here to learn more about Vulnerability & Patch Management

© 2023 Lookout, Inc. LOOKOUT®, the Lookout Shield Design®, LOOKOUT with Shield Design®, and SIGNAL FLARE® are registered trademarks of Lookout, Inc. in the United States and other countries. DAY OF SHECURITY®, LOOKOUT MOBILE SECURITY®, and POWERED BY LOOKOUT® are registered trademarks of Lookout, Inc. in the United States. Lookout, Inc. maintains common law trademark rights in EVERYTHING IS OK, PROTECTED BY LOOKOUT, CIPHERCLOUD, SCREAM, the 4 Bar Shield Design, and the Lookout multi-color/multi-shaded Wingspan design.