



Adobe Acrobat Reader



Overview

There has been a critical vulnerability found in Acrobat Reader for Android devices that could enable an unauthorized user to execute arbitrary code executing on the user's device. The vulnerability, [CVE-2021-40724](#), was given a score of 7.8 by NIST, seems to affect all versions of the app before 21.9.0. The patched version of the app is now available in the Google Play store, and every vulnerable user should update to the latest version of Adobe Reader for Android as soon as possible.

Arbitrary code execution (ACE) is a significant risk to any vulnerable device, the apps on it, and the data it has access to. ACE vulnerabilities enable the attacker to run any command or code they desire on the targeted device. For this vulnerability, NIST notes that "exploitation of this issue requires user interaction in that a victim must open a malicious file." With that being the case, attackers would most likely deliver the file as a malicious attachment in socially engineered outreach to a target.

Lookout Coverage and Recommendation for Admins

Admins should ensure that the default vulnerable app policy is enabled in the *Protections* page of the Lookout console. Any vulnerable version of Adobe Acrobat will be classified as a threat, so all users with a vulnerable version will receive an alert as well as guidance on how to update from Lookout on their device. In addition, admins can denylist any version of Adobe Acrobat for Android before 21.9.0.

Lookout Analysis

Adobe Acrobat is a very popular app in the enterprise setting, which means attackers may focus on creating social engineering campaigns that have a corporate angle. The security research community has noted threat actors are more frequently launching sharing malicious files through social engineering on collaboration platforms like Google Drive and Dropbox. With arbitrary code execution, the attacker may use this tactic to exploit the vulnerability and run code that puts corporate data at risk. Other tactics for delivering malicious files include sharing in on social media platforms, professional networking apps, and third-party messengers.

Lookout Threat Advisory Service

In the fast-changing world of mobile security, keeping your finger on the pulse can be challenging. Lookout Threat Advisory taps into the massive dataset from Lookout's global sensor network of millions of devices, pairing it with insight from its top security researchers to give you actionable intelligence on the latest mobile threats and risks.

[Click here to learn more about Lookout Threat Advisory](#)