Hackers can steal 2FA codes and private messages from Android phones

Android devices are vulnerable to a new attack that can covertly steal two-factor authentication codes, location timelines, and other private data in less than 30 seconds.

The new attack, named Pixnapping by the team of academic researchers who devised it, requires a victim to first install a malicious app on an Android phone or tablet. The app, which requires no system permissions, can then effectively read data that any other installed app displays on the screen. Pixnapping has been demonstrated on Google Pixel phones and the Samsung Galaxy S25 phone and likely could be modified to work on other models with additional work. Google released mitigations last month, but the researchers said a modified version of the attack works even when the update is installed.

Like taking a screenshot

Pixnapping attacks begin with the malicious app invoking Android programming interfaces that cause the authenticator or other targeted apps to send sensitive information to the device screen. The malicious app then runs graphical operations on individual pixels of interest to the attacker. Pixnapping then exploits a side channel that allows the malicious app to map the pixels at those coordinates to letters, numbers, or shapes.

“Anything that is visible when the target app is opened can be stolen by the malicious app using Pixnapping,” the researchers

wrote on an informational website. “Chat messages, 2FA codes, email messages, etc. are all vulnerable since they are visible. If an app has secret information that is not visible (e.g., it has a secret key that is stored but never shown on the screen), that information cannot be stolen by Pixnapping.”

The new attack class is reminiscent of GPU.zip, a 2023 attack that allowed malicious websites to read the usernames, passwords, and other sensitive visual data displayed by other websites. It worked by exploiting side channels found in GPUs from all major suppliers. The vulnerabilities that GPU.zip exploited have never been fixed. Instead, the attack was blocked in browsers by limiting their ability to open iframes, an HTML element that allows one website (in the case of GPU.zip, a malicious one) to embed the contents of a site from a different domain.

https://arstechnica.com/security/2025/10/no-fix-yet-for-attack-that-lets-hackers-pluck-2fa-codes-from-android-phones/