

通信・ITネットワークの分野では、日々新しい技術が開発され、より効率的で、より安価なサービスが次々と生み出されています。知らないことは、イコール企業利益の損失です。そこで私たち大和電設工業は、情報通信やITソリューションの『知って得する最新情報』を、お世話になっている皆様に定期的にお伝えしていきます。隔月発刊のDDK通信、ぜひお楽しみください。

Androidスマホを「見ているだけ」で情報流出？

ビジネスでもスマートフォンを使う機会が増えてきて、業務情報や顧客情報、社内システムの情報など、多くの重要な情報がスマホの画面に表示されています。悪意あるハッカーにその画面の内容を知らないうちに盗み見られるような事があれば、重大な情報が外

部に流出する事故になってしまいます。そんな危険なことが、Androidスマホで起こり得る事案が2025年10月に発表されました。あなたのお使いのAndroidスマホは大丈夫ですか？

悪質なハッキングの手口とは？

今回新たに発見されたハッキングの手口は「**Pixnapping(ピクスナッピング)**」と呼ばれる技術で、スマホ画面を構成する最小単位であるピクセルの情報を、画面表示に関わる信号の時間差を読み取り、表示される内容を推察する手口です。画面のキャプチャやスクリーンショットとは異なり、直接的に画像データを取得するわけではないため、ユーザーに警告通知を出したり、検知したり

することが難しいと考えられています。

ユーザーがアプリを使っているとその裏で情報を読み取っているの、権限や制限を設定して防ぐことも困難です。また、他のアプリと一緒にインストールされる形で端末内に潜入する可能性があると考えられています。その為、スマホや利用中のアプリに存在する脆弱性を放置しておくことは思わぬ情報漏洩のリスクにつながりかねません。

Pixnapping(ピクスナッピング)対策

このハッキング手口は、2013年にイギリスの研究者によってWebブラウザ上の攻撃として既に報告され、完全に防御されていました。昨年10月には、カリフォルニア大学やワシントン大学など米国の複数の大学の研究チームが、Android端末においてもPixnappingによる被害の可能性があることを発表しました。

Googleはすぐにこの脆弱性を「高リスク」と評価し、対応策として「被害を軽減するために、アプリが呼び出せる活動の数を制限」しました。しかし、研究者たちはその修正のわずか2日後に回避策を考案したと報告しています。

悪意あるアプリをインストールしてしまった場合、一般ユーザーが個別に防ぐことは困難です。記事執筆時点では、対策パッチの提供状況を明確に確認できていませんが、今後順次対応が行われる予定になっています。その為、スマートフォンのセキュリティアップデートを常に最新の状態に保つようにご確認下さい。

被害を受ける可能性のある端末

この脆弱性を発見した研究チームは、Google Pixel 6~9やAndroidバージョン13~16を搭載したSamsung Galaxy S25など、複数の主要端末でPixnappingによる攻撃を実証し、いずれも新たなサイドチャンネル攻撃に対して脆弱であることを確認しました。

こうした結果は、広く流通する端末の多くが同様のリスクにさらされていることを示しており、ユーザーはOSの更新を速やかに適用すること、また開発者側も端末やアプリのセキュリティ強化に注力することが重要であることを改めて浮き彫りにしています。

今後も新たな攻撃手法が登場する可能性は否定できず、日頃から情報セキュリティに対する意識を高めることが、モバイル端末を安全に使い続けるための最も確実な対策と言えるのかもしれません。

