„VHS-Problem“ sorgt für grafische Datenpannen

Bildbearbeitungsprogramme bei Google Pixel und Windows 11 geben mehr preis als gewünscht. Das müssen Nutzer jetzt wissen, um persönliche Daten zu schützen.

Berichte über einen Bug in den Bildbearbeitungsprogrammen Markup bei den Google-Pixel-Telefonen und „Snipping Tool“ bei Windows 11 sorgen zurzeit für Schlagzeilen. Das Problem kann im besten Fall zu witzigen womöglich aber auch peinlichen Ergebnissen führen: statt unerwünschte Informationen aus einem Bild herauszuschneiden (Gesichter, Kennzeichen etc.), bleiben sie enthalten – ein Problem, wenn man diese irrtümlich „neutralisierten“ Fotos weiterverbreitet.
Paul Ducklin von Sophos erklärt das Prinzip des „Überschreibens“ anhand der guten alten VHS-Kassette und gibt Sicherheitstipps für Nutzer.

Das VHS-Prinzip – Überschreiben von Altem, mit merkwürdigen Resten
Der Bildbearbeitungs-Bug beschreibt ein Phänomen, das viele von uns noch aus der Ära der VHS-Kassetten kennen: Man gehe von einer VHS-Kassette mit Lauflänge 60 Minuten aus, die Fernsehsequenz, die man aufnehmen wollte, lief aber nur 45 Minuten (besser als umgekehrt). Im Idealfall war die Kassette neu und damit unbespielt und es blieb einfach nur ein „Rauschen“, wenn der Nutzer das Band nach dem Ende der Sendung laufen ließ, bis der Videorekorder das Ende der Spule erkannte und die Kassette für das nächste Mal zurückspulte.

Im Fall einer bereits bespielten Kassette allerdings wird der Nutzer sich den letzten Teil von dem ansehen, was von der vorherigen Aufnahme übriggeblieben war und wenn diese zu Ende war, das, was davor aufgenommen wurde, oder die Zeit davor, und so weiter. Wenn nicht zuerst das gesamte Band gelöscht wurde, bevor es neu bespielt wurde, blieben fast immer unerwartete und vielleicht unerwünschte Inhalte am Ende übrig.

So ähnlich verhält es sich auch mit dem Fehler in den Bildbearbeitungsprogrammen von Windows 11 sowie der Google-Pixel-Telefone.

Kodierungsfehler in der Software – der Rattenschwanz bleibt
Die beanstandete Software-Markup von Google Pixel zum Beispiel ermöglicht es, Fotos oder Screenshots, die sich bereits auf dem Nutzer-Telefon befinden, zu beschneiden oder anderweitig zu bearbeiten, um unerwünschte Details wie Benutzernamen, Konto-ID, Gesichter, Kennzeichen etc. zu entfernen, bevor man sie an Freunde senden oder auf Online-Diensten hochladen kann.

Bis vor rund zwei Jahren hat Markup kleinere Bilder bearbeitet, indem es das neue Bild über das alte geschrieben und dann die Bilddatei auf die neue, kürzere Größe abgeschnitten hat. Die alten Daten – in unserer Videorekorder-Analogie das Ende des Vorher-Aufgenommenen – blieben auf dem Speichergerät zurück, aber sie waren nicht mehr Teil der digitalen Datei, die das neue Bild enthält.

Mit anderen Worten: Öffnete der Nutzer die neue Datei, hatte er nicht das alte Problem der Bildreste wie beim Videorekorder, denn das Betriebssystem wusste, dass es das Lesen (oder Kopieren) der Datei an der richtigen Stelle beenden muss.

Ein Angreifer bräuchte so normalerweise physischen Zugang zu dem Telefon, müsste wissen, wie man es entsperrt und Root-Rechte erhält, um in der Lage zu sein, ein forensisches Abbild der ungenutzten Daten zu erstellen, um alle zuvor gelöschten Daten wiederherzustellen.

„Öffnen im Überschreibmodus ohne Abschneiden nach Abschluss“
Wie mittlerweile bekannt ist, wurde die Java-Programmierfunktion in Markup vor rund zwei Jahren in „Öffnen im Überschreibmodus ohne Abschneiden nach Abschluss“ geändert. Das, was man also vielleicht herauslöschen möchte, bleibt stur erhalten! Damit können die meisten zwar nichts anfangen, aber einige Findige (mit womöglich unsauberen Absichten) dennoch.

Was sollte man jetzt tun?

1. Patchen
Google hat ein Sicherheitsupdate für Android veröffentlicht, die Kennung lautet CVE-2023-20136.

2. Überprüfen der bereits freigegebenen Bilder
Überprüfen Sie Bilder, die Sie bereits freigegeben haben. Für Bilder, die Sie bereits beschnitten und freigegeben haben, ist es zu spät, um sie zu korrigieren. Sie sollten jedoch in Erwägung ziehen, sie trotzdem zu entfernen oder sie durch neu bearbeitete Bilder zu ersetzen, die mit der gepatchten Version von Markup erstellt wurden.

3. Bilder lieber konservativ bearbeiten
Eine Überlegung ist, sicherheitskritische Bilder auf dem Laptop lieber konservativ zu bearbeiten. Dateiformate wie PNG (Portable Network Graphics) können auch Kommentare und so genannte Metadaten (z. B. Standortinformationen oder Kameradetails) enthalten, die opak bleiben sollten.
Befehlszeilen-Tools zur Bildbearbeitung wie ImageMagick oder GraphicsMagick und Open-Source-Tools wie das GNU Image Manipulation Program ermöglichen es, bearbeitete Bilder in Formate zu konvertieren, bei denen sich der Inhalt genau kontrollieren lässt.

RGB-Rohdateien beispielsweise enthalten nur die Farbwerte jedes Pixels im Bild, ohne Kopfzeilen, Metadaten, Kommentarfelder oder andere Fremdinformationen oder Pixel.

Die Transkodierung eines Bildes in das RGB-Format und dann wieder zurück, z. B. in PNG, ist also eine Möglichkeit, um sicherzustellen, dass der Nutzer eine völlig neue Datei erstellt, die nichts darüber „weiß", wo oder wie das ursprüngliche Bild erstellt wurde oder welche nun gelöschten Daten es zuvor enthalten haben könnte.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198