Summary

The Snipping Tool has led to privacy risks despite the convenience of inbuilt software. According to Abrams (2023), security researchers discovered a privacy flaw named 'acropalypse' that affects the Windows Snipping Tool by partially recovering edited or cropped images. Privacy leaks occur when we edit or crop an image file and overwrite it with an existing one, leaving untruncated data behind. This allows attackers to recover the image partially. It also risks users who frequently share privacy-related images. Even if the pictures are edited or cropped, they still pose a risk of recovering the vital information in the photo (Abrams, 2023). As a result, it suggests the challenge of maintaining user and company confidentiality and privacy when taking screenshots of sensitive content or documents meant to remain private. Microsoft is actively investigating the issue to mitigate the problem and enhance user safety with security updates. Alongside technical solutions, Microsoft may also provide guidelines by raising public awareness. They should provide guidelines for users and emphasise saving images as new files instead of overwriting existing ones, ensuring that the image becomes impossible to recover (Abrams, 2023). In conclusion, software developers and users must cooperate and be aware of this issue to prevent attackers from achieving their purposes.

Identification of affected software, hardware or system

The bug mainly affects in-built software of the operating systems Windows 10 and Windows 11. For Windows 10, the software is named "Snip and Sketch" (version below 10.2008.3001.0), and for Windows 11, the software is named "Snipping Tool" (version below 11.2302.20.0) (Endicott, 2023). The main problem is how the software cop with data truncation when overwriting existing image files, as the untruncated data is the primary cause of allowing edited images to be recovered.

Description on how the problem was discovered and initially published.

The "acropalypse" flaw was first found in Google Pixel's Markup tool by security researchers that it is possible to recover information from an edited image (Toulas, 2023). This creates awareness among all cybersecurity professionals on how this problem works. A day later, the privacy flaw was also found to affect the Windows 11 Snipping Tool (Abrams, 2023). image file, both in PNG file type. Although the image viewer correctly shows the cropped and original versions, both files have the same size, which is illogical. Apart from that, according to PNG file specification, a PNG image file must ends with an 'IEND' data chunk (Abrams, 2023). Any data added after that will be disregarded. However, when the user overwrites the

original image with the cropped version, the image contains two 'IEND' data chunks and continues with nearly all of the image data from the old file (Ducklin, 2023). Then, a Python script was used to recover cropped image files. It partially reconstructed the original image due to the untruncated data. In short, it does not exactly replaced the existing file.

Discussion on seriousness of the issue and useful actions

The issue has a significant impact on causing users to lose confidentiality. Partially recovering the edited image may cause the original data intended to be kept private and removed to be exposed to unauthorised parties. The attacker can recover the images by having cropped PNG image files to exploit the weakness. From the image files, several tools help recover, such as acropalypse.app, to obtain confidential data (Amadeo, 2023). If the users expose the cropped image of credit card information, it poses a high chance for hackers to recover the part of the image that consists of crucial private information. In this case, exploiting the weakness will result in unauthorised access to private data and severely lead to possible bank fraud, such as identity theft and phishing.

Therefore, responsible authorities must take appropriate measures to solve this issue. From a technical level, Microsoft, as the software developer of Windows OS, should release a patch to inform users, followed by an update on removing untruncated data (Endicott, 2023). Moreover, they can also implement image encryption techniques such as Steganography by adding an extra layer of protection (Badra, 2023). This technique allows us to hide the original photo within the cropped image, ensuring the original photo remains safeguarded through encryption. Next, users who frequently use the software must be extra cautious when sharing images. Most importantly, save the cropped image as new file name to prevent overwriting the file, resulting in untruncated data (Ducklin, 2023). Last, policymakers such as governments and national bodies should establish cybersecurity policies and regulation with strict penalties on illegal actions such as data breaches. Cybersecurity education in primary education would allow citizens to make correct judgements and use the Internet.

References

Abrams, L. (2023, March 21). Windows 11 Snipping Tool privacy bug exposes cropped image content. *BleepingComputer*. https://www.bleepingcomputer.com/news/microsoft/windows-11-snipping-tool-privacy-bug-exposes-cropped-image-content/

Amadeo, R. (2023, March 20). Google Pixel bug lets you "uncrop" the last four years of screenshots. *Ars Technica*. https://arstechnica.com/gadgets/2023/03/google-pixel-bug-lets-you-uncrop-the-last-four-years-of-screenshots/#:~:text=It

Badra, H. (2023, August 23). *How to Build a Photo Encryption App using Steganography*. *freeCodeCamp.org*. https://www.freecodecamp.org/news/build-a-photo-encryption-app/

Ducklin, P. (2023, March 22). Windows 11 also vulnerable to "aCropalypse" image data leakage. *Sophos News*. https://news.sophos.com/en-us/2023/03/22/windows-11-also-vulnerable-to-acropalypse-image-data-leakage/

Endicott, S. (2023, March 27). Windows 11 Snipping Tool "aCropalypse" bug fixed with emergency update from Microsoft. *Windows Central*. https://www.windowscentral.com/software-apps/windows-11/windows-11-snipping-tool-acropalypse-bug-fixed-with-emergency-update-from-microsoft#:~:text=The%20bug%20only%20affects%20Snip

Toulas, B. (2023, March 20). Google Pixel flaw allowed recovery of redacted, cropped images. *BleepingComputer*. https://www.bleepingcomputer.com/news/security/google-pixel-flaw-allowed-recovery-of-redacted-cropped-images/