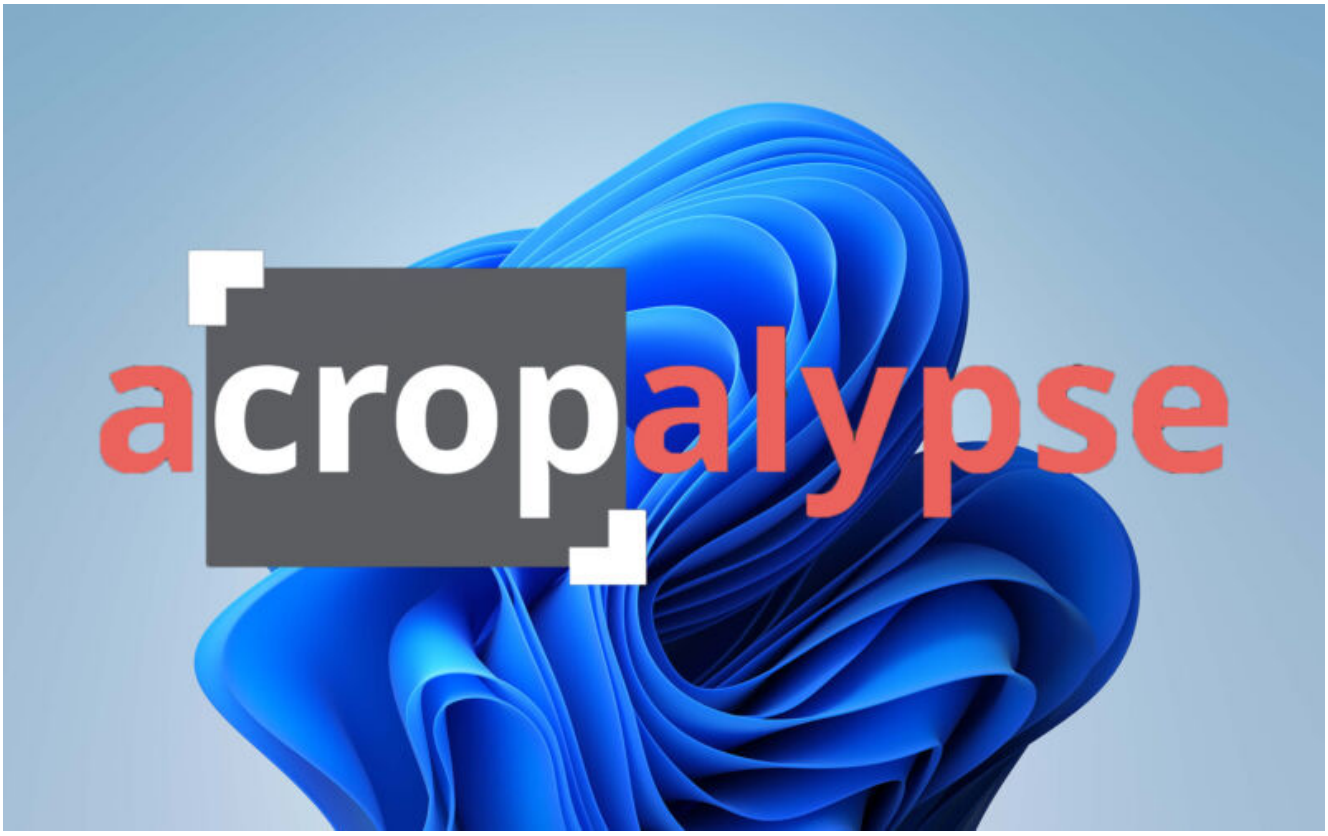
“Acropalypse” Android screenshot bug turns into a 0-day Windows vulnerability



Enlarge / Windows 10 and 11 have their own version of the Acropalypse screenshot editing bug.
acropalypse.app/Andrew Cunningham

reader comments

49 with

Share this story

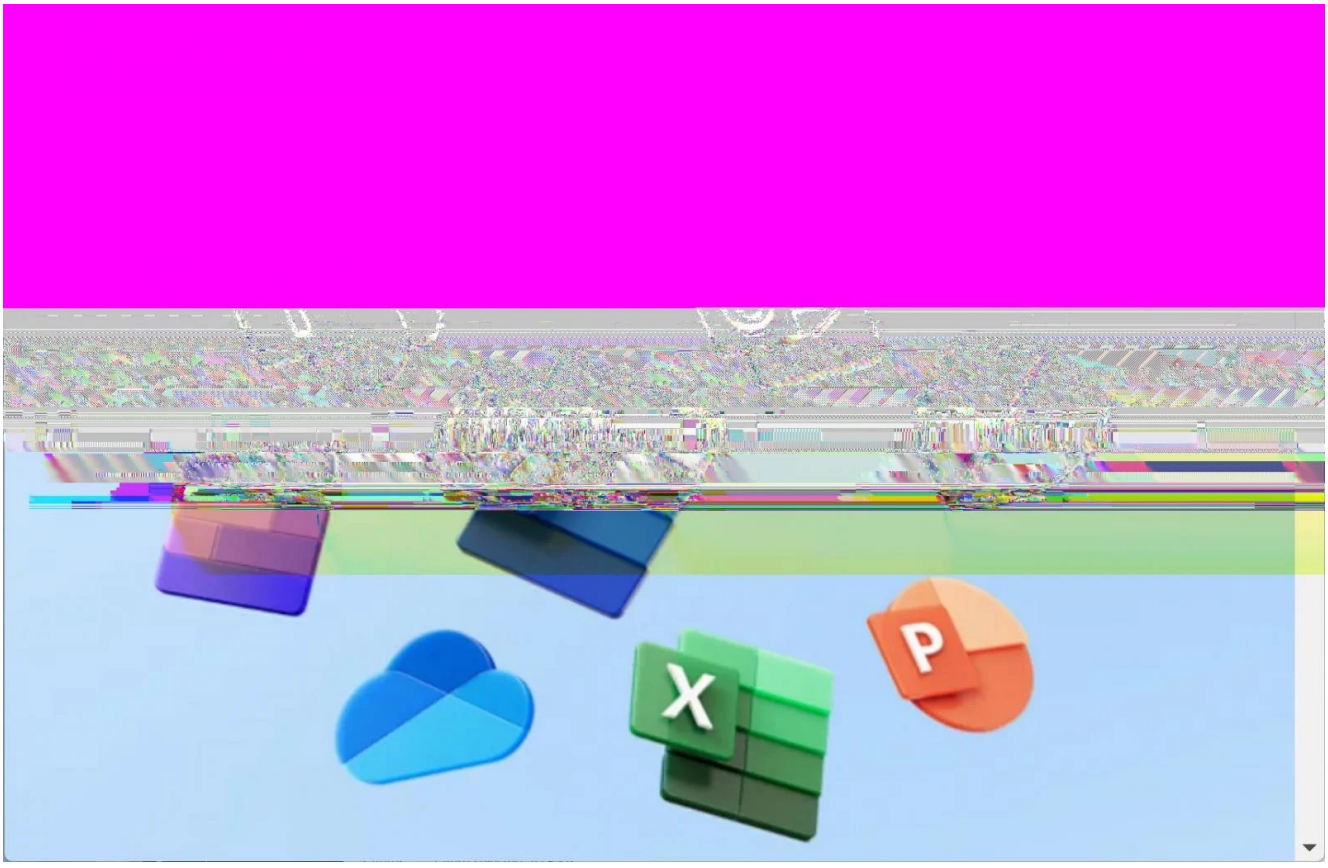
Earlier this week, programmer and “accidental security researcher” Simon Aarons disclosed a bug in Google’s Markup screenshot editing tool for its Pixel phones. Dubbed “acropalypse,” the bug allows content you’ve cropped out of your Android screenshot to be partially recovered, which can

be a problem if you've cropped out sensitive information.

Today, Aarons' collaborator, David Buchanan, revealed that a similar bug affects the Snipping Tool app in Windows 11. As detailed by Bleeping Computer, which was able to verify the existence of the bug, PNG files all have an "IEND" data chunk that tells software where the image file ends. A screenshot cropped with Snipping Tool and then saved over the original (the default behavior) adds a new IEND chunk to the PNG image but leaves a bunch of the original screenshot's data *after* the IEND chunk.

Advertisement

Buchanan says that a version of the acropalypse script "with minor changes" can be used to read and recover that data, partially restoring the part of the image you cropped out of your original screenshot. Buchanan is "holding off on publishing" Windows-compatible versions of those scripts since Microsoft (unlike Google) hasn't had time to patch the vulnerability.



A Windows screenshot that has been cropped and then partially

recovered using a modified version of the acropalypse script. Not all of the image is recoverable, but this could still potentially expose confidential information.
Buchanan says the issue also affects the “Snip and Sketch” tool in Windows 10, the app that became the basis of the new Windows 11 Snipping Tool. The old Windows Vista-era Snipping Tool, still included as a separate app in Windows 10, isn’t affected by the bug.

Microsoft told Bleeping Computer that it was “investigating” the problem. In the meantime, there are workarounds—re-saving your cropped image with another photo-editing app does appear to fully strip out the data from the end of the file. And while the Snipping Tool does appear to leave data at the end of cropped JPEG files, current exploits only work with PNG images, not JPEGs.

https://arstechnica.com/?p=1925853