A reported vulnerability about getting paid apps for free is really about paying for free apps

devblogs.microsoft.com/oldnewthing/20231128-00

November 28, 2023

Raymond Chen

A security vulnerability report arrived showing how it is possible to get paid apps for free from the Microsoft Store.

- Open the Microsoft Store app and search for WinSCP.
- Observe that there are three versions of WinSCP in the Store, one selling for $9.99 and another for $4.59, and another for $6.69.
- Go to a command prompt and type `winget install WinSCP`
- Observe that WinSCP is installed without requesting payment.

The vulnerability report was actually much longer, but it consisted mostly of breathless prose saying how this vulnerability could result in disclosure of confidential information by employees who use the program to transfer files, some of which might be malicious.

Okay, first, let's address the breathless prose: It's like saying, "The customer bought printer paper from your office supply store. The customer might use that paper to print a confidential document and then smuggle it out of the building. This is a security vulnerability in your office supply store!" I mean, the customer bought the paper fair and square. They used valid funds, not tied to a stolen credit card. It's not the office supply store's fault that the paper could be used to print a confidential document that is smuggled out of the building. And even without printer paper, the customer could use their camera to take a picture of a confidential document. And if the employees don't install WinSCP, they can still disclose confidential information by emailing the documents instead of using WinSCP to transfer them. It's not clear how it's the fault of Windows that a rogue employee can use WinSCP to disclose confidential information.

As for the issue of installing paid software for free: Look again at the program in question. WinSCP is actually free software. Go to the home page, and right there top and center it says "Free Award-Winning File Manager", and under it is a big green *Download Now* button.

What you're seeing is people taking this free software, repackaging it, and trying to sell it. Repackaging WinSCP is explicitly supported, providing the redistribution adheres to the WinSCP license.

One of those repackaged WinSCP apps is in fact the official one from the author of WinSCP. You can buy it from Martin Prikryl to provide financial support to the WinSCP project.

The other two WinSCP apps look sketchier. For example, they list English as the only supported language, yet the privacy policy is written in Chinese. And looking at other offerings from those publishers suggests that their portfolios consist of repackaged free software. I didn't do a thorough analysis, but I checked two other offerings from those publishers and they were both software that was already free to download directly from the original authors.

The finder should have been suspicious when there were *three* copies of the product in the Store from different publishers. Why would a piece of software have three publishers?