Summary

Two researchers – Eyal Itkin & Yaniv Blamas from Check Point Research successfully exploited an HP all- in-one printer by sending it a “malicious” fax.

In other words, they were able to send a fax to a specific type of HP printer and have that printer execute code (contained in the fax) that could possibly infect and take control of other computers on a network the HP printer was connected to.

Is Cleo Streem Server Vulnerable?

No.

Why Not?

1. We do not use HP all-in-one printers to receive faxes.
2. We do not use any HP software/hardware to receive faxes.
3. This exploit is only *remotely* possible when receiving color faxes and currently there are zero Cleo Streem customers using color faxing.

Technical Details

1. This vulnerability exploited the fact that HP used a “simple” internally written jpeg parser (they didn’t use libjpeg)
2. Streem uses libjpeg to convert color faxes (when color faxing is enabled) to .tiff/.pdf for delivery (email, print, lpr) to the end user.
3. Currently, there are zero known CVE’s open on libjpeg that allow code execution. Past fixed CVE’s simply allowed DOS (Denial of Service) which simply meant a program using it might crash.
4. We have a single program (img2tif.exe) which pre-processes received image for delivery to intended recipients.
    a. Img2tiff uses the latest version of an OSS library named “FreeImage” which in turn uses libjpeg for processing (reading/writing) jpeg images.
    b. There are zero known open CVE’s related to FreeImage

Exploit Details

https://research.checkpoint.com/sending-fax-back-to-the-dark-ages/