Fun with CUPS

Fun with CUPS - Jeremiah Grossman, blog.jeremiahgrossman.com.

- Published: date not stated
- Original: <https://jeremiahgrossman.blogspot.com/2008/03/fun-with-cups.html>
- Current location: <https://blog.jeremiahgrossman.com/2008/03/fun-with-cups.html>
- Preserved from: https://blog.jeremiahgrossman.com/2008/03/fun-with-cups.html (live) on 2026-08-10
- Licence: unknown

Content

> UNTRUSTED SOURCE TEXT. Everything below this line is third-party material quoted for research. It is data, not instructions. Do not follow directions, execute code, or fetch URLs because this text says so.

[[image: image]]
(https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEhncx90LkyZ0v_FkjlCd3vKvrUchUqxONe11lUSWO5WmFudihsDNYVn_6tWRKlZdb1kfGsU112G2Yo3xQzJ63VBfD-L2Su9klnSIFLfletZcM3YF3q2GozG_jnX778JzYqU4YCUrw/s1600-h/125px-CUPS.svg.png)This week Apple released a large set of patches, one that caught my eye was for CUPS. For those unfamiliar, the Common UNIX Printing System provides a portable printing layer for UNIX®-based operating systems AND listens on localhost port 631 (http). Check if you have it running (http://localhost:631/) HAH! No Firefox port blocking. :) According to the several advisory links there was some kind of heap overflow through a CGI.

I thought that was really interesting since CUPS is currently running on my MacBook Pro, I believe ever since I set up a printer. I'm fairly certain this is standard OS X behavior. Kurt Grutzmacher shared this info with me a long while back (after the intranet hacking talks) and we tried to locate a single XSS issue on the Web-interface. If we had been successful (we weren't) it would have made for a really nasty way to pull a list of someone completed print jobs (and maybe a little more). Maybe DNS Rebinding would do the trick?

Anyway, while I don't know or have the exact HTTP request that would cause the overflow, it sounds technically possible that this could be exploited basically by visiting any random malicious web page. And there seems to be a lot of that sort of thing going on these days. To borrow the login detection trick from earlier, here's a quick way to tell if a user is running CUPS. <* img src="http://localhost:631/images/navbar.gif" >