



Issued 8/11/17

US Court System Bug Opened Hole for Hackers to Scoop Up Legal Docs for Free on Victims' Dime

A cross-site forgery vulnerability in the American court system's document archive PACER has been fixed. The bug could have been exploited to hijack accounts and retrieve civil and criminal lawsuit files on victims' dime. PACER, run by the Administrative Office of the US Courts, is a massive searchable trove of records, exhibits, indictments, complaints and more, on legal battles working their way through America's courtrooms. It's mainly used by lawyers and journalists, and costs 10 cents a page when pulling up PDFs and webpages of files, up to three bucks per document.

The Free Law Project says the cross-site forgery flaw could have allowed an attacker to set up a website that would be able to harvest the PACER account credentials of anyone who visited. This information could be used to download PDFs, charging the victims cash in the process. According to the researchers, the flaw stems from PACER's use of cookies to store login credentials. Because those cookies are not securely handled, any site would be able to call them up and retrieve the visitor's PACER login details with just a bit of JavaScript. The researchers have presented a proof of concept to demonstrate the flaw,

but say it was not exploited in the wild prior to being published. "For users of PACER, unpaid fees can result in damage to their credit, and debt collectors sent to their door at the behest of the Administrative Office," the researchers explain. "They would never know why their PACER bill skyrocketed." What's worse, researchers say the vulnerability has likely been around since the 1990s, when PACER first went online.

The Free Law Project says it reported the issue in February, and it was finally fully fixed on Wednesday this week.