RelianceCyber

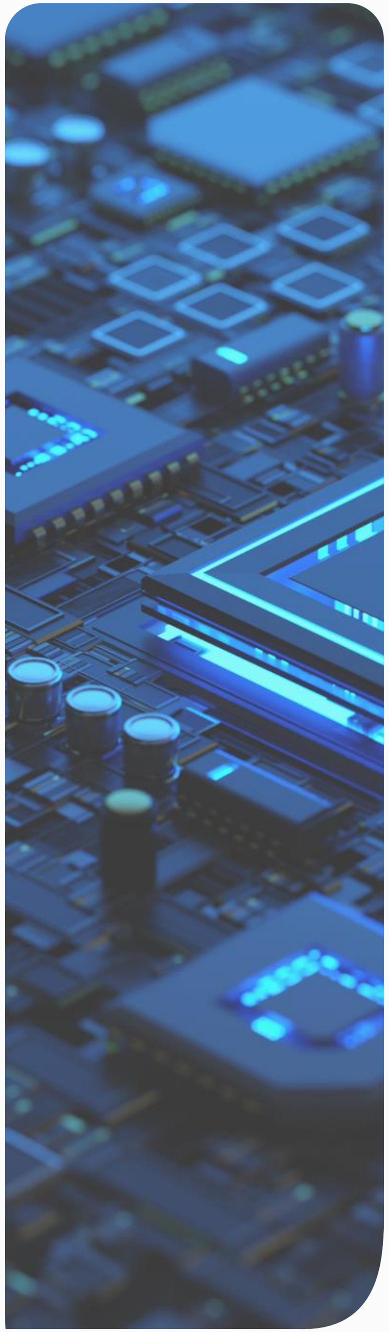
TLP: CLEAR

Threat Intelligence

Threat Advisory

Written by: Adam Schweizer

Date: 2024-09-27



Threat Advisory – Common UNIX Printing System (CUPS) Vulnerabilities

Summary	Multiple vulnerabilities were found in the Linux open-source printing systems that, if exploited, could lead to arbitrary remote code execution. OpenPrinting CUPS is prevalent in most modern Linux distributions. Simone Margaritelli recently disclosed the following vulnerabilities - CVE-2024-47076 (libcupsfilters), CVE-2024-47175 (libppd), CVE-2024-47176 (cups-browsed) and CVE-2024-47177 (cups-filters). Proof of concept is available here. Despite these vulnerabilities affecting most Linux distributions, exploiting them required a very specific chain of events (Exploitation) which is not trivial.
CVSSv3	8.4 – 9.1
Exploited in the Wild	No
Affected Technology and Version	Most Linux distributions are suspected to be affected by these vulnerabilities, it is best to follow the steps below. Red Hat Enterprise Linux (RHEL) confirmed that default configurations are not impacted. Use the following command to determine if cups-browsed is running (RedHat): • **sudo systemctl status cups-browsed**
Recommendations	• Use the following commands to stop the services **sudo systemctl stop cups-browsed** (stop a running cups-browsed service) **sudo systemctl disable cups-browsed** (System will prevent starting the cups-browsed service on reboot) • Remove cups-browsed • CUPS is set to listen on UDP port 631, so it is advised to block all traffic to UDP port 631.
Sources	https://www.bleepingcomputer.com/news/security/cups-flaws-enable-linux-remote-code-execution-but-theres-a-catch/ https://www.evilsocket.net/2024/09/26/Attacking-UNIX-systems-via-CUPS-Part-I/#Summary https://www.redhat.com/en/blog/red-hat-response-openprinting-cups-vulnerabilities https://www.tenable.com/blog/cve-2024-47076-cve-2024-47175-cve-2024-47176-cve-2024-47177-faq-cups-vulnerabilities

RelianceCyber

RELIANCECYBER.COM