Silent Print, Loud Threat: Exploiting CUPS Vulnerabilities in UNIX Systems

---

1. Vulnerability Identification:

- **Relevant CVEs**:
  - **CVE-2024-47176**: Affects the cups-browsed daemon. Allows attackers to send malicious IPP requests leading to arbitrary code execution when a print job is initiated (Cybersecurity News)(Enterprise Technology News and Analysis).
  - **CVE-2024-47076**: Impacts libcupsfilters, where unsanitized IPP attributes can be processed by CUPS, leading to code execution (Rapid7).
  - **CVE-2024-47175**: Involves libppd allowing malicious IPP data to create vulnerable PPD files (BleepingComputer).
  - **CVE-2024-47177**: Exploits the foomatic-rip filter in CUPS, leading to arbitrary command execution via the FoomaticRIPCommandLine (Rapid7).
- **Affected Systems**: Linux, UNIX-like operating systems, FreeBSD, OpenBSD, and Oracle Solaris systems using vulnerable versions of CUPS.
- **Exploitability**: Proof of Concept (PoC) code is available for CVE-2024-47176 (Cybersecurity News), and the vulnerability can be exploited via network-based attacks (UDP 631) or local exploitation.
- **CVSS Scores**: While initial estimates suggested a **9.9 severity**, the real-world impact is lower due to mitigations like disabled services by default (BleepingComputer).

---

2. Exploit Availability and Exploitability:

- **Exploit Vector**: Attackers can exploit stack buffer overflows and race conditions within the CUPS architecture, including using foomatic-rip and IPP for remote command execution.
- **Exploit Kits**: PoC for CVE-2024-47176 is available(Cybersecurity News), and exploits are shared in forums, GitHub, and Shodan data shows over 75,000 hosts running CUPS exposed (Rapid7)(BleepingComputer).
- **MITRE ATT&CK TTPs**: T1189 (Drive-by Compromise), T1071.001 (Application Layer Protocol).

---

3. Risk Assessment and Prioritization:

- **CVSS Scores**: Based on the vulnerabilities' potential for RCE, CVSS scores range from **9.9** for CVE-2024-47176 (overestimated) to **Important** based on mitigations (Enterprise Technology News and Analysis).
- **Likelihood of Exploitation**: Moderate, given that systems must have cups-browsed enabled and exposed to exploit. However, PoCs and public interest in these vulnerabilities are high.

- **Business Impact**: Vulnerabilities could compromise sensitive print jobs or serve as a pivot point for network attacks, impacting internal operations or compliance.

---

4. Affected Assets and Attack Surface:

- **Systems Impacted**: Linux and UNIX-like systems with CUPS enabled, specifically those with cups-browsed listening on UDP port 631.
- **Configurations Increasing Risk**: Systems with internet-facing CUPS services, default or legacy configurations using vulnerable components such as foomatic-rip (BleepingComputer).

---

5. Remediation and Mitigation Actions:

- **Official Patches**: Patches are under development but not yet fully released. Some mitigations include stopping and disabling cups-browsed and blocking traffic to UDP port 631 (Cybersecurity News)(Enterprise Technology News and Analysis).
- **Temporary Workarounds**:
  - Disable cups-browsed: sudo systemctl stop cups-browsed and sudo systemctl disable cups-browsed.
  - Block UDP 631: iptables -A INPUT -p udp –dport 631 -j DROP.
  - Monitor for patches from vendors like Canonical, Red Hat (Cybersecurity News).

---

6. Exploitation Scenarios and Case Studies:

- **Real-World Impact**: While no major public incidents have been reported yet, researchers have flagged the vulnerabilities as dangerous due to the large attack surface exposed by CUPS, particularly in enterprise environments (Enterprise Technology News and Analysis).

---

7. Threat Actor Profiling:

- **No Specific Attribution**: The vulnerabilities will likely attract cybercriminals and APT groups interested in exploiting networked infrastructure like printers (Enterprise Technology News and Analysis).

---

8. Detection and Monitoring Guidance:

- **SIEM Rules**: Monitor traffic on UDP port 631 for unusual print jobs or unexpected printers. Also, monitor logs from CUPS for suspicious requests and exploits involving foomatic-rip (Cybersecurity News).
- **Indicators of Compromise (IOCs)**: IPs and commands used in the exploitation of foomatic-rip and IPP-related vulnerabilities.

---

9. Continuous Vulnerability Management:

- **Recommended Tools**: Automate CUPS vulnerability scanning using tools like Nessus, OpenVAS, or proprietary vulnerability management solutions that can detect unpatched services.

---

10. Vulnerability Correlation and OSINT Findings:

- **Ongoing Campaigns**: The high exposure of internet-facing CUPS systems and availability of PoCs indicate a likely increase in exploitation attempts (Rapid7).

---

11. Compliance and Regulatory Considerations:

- **Regulatory Impact**: Failure to patch these vulnerabilities could lead to non-compliance with PCI-DSS or other regulatory frameworks depending on the environment (Enterprise Technology News and Analysis).

---

12. Collaboration and Third-Party Risk:

- **Vendor Coordination**: Work closely with vendors like Canonical, Red Hat, and third-party service providers using CUPS to ensure timely patching and mitigation of vulnerabilities(Cybersecurity News)(Enterprise Technology News and Analysis).

---

13. Lessons Learned and Future Prevention:

- **Hardening Systems**: Disable unused services like cups-browsed, restrict network access to sensitive printers, and enforce strict patch management protocols to prevent future exploits(BleepingComputer).