Four CUPS Vulnerabilities Expose Linux and Unix Systems to Remote Code Execution (RCE)

Overview

Four zero-day vulnerabilities were found in the Common UNIX Printing System (CUPS), impacting Linux and Unix-like systems. These vulnerabilities allow remote, unauthenticated attackers to execute arbitrary code by exploiting misconfigurations in CUPS components. Affected systems include popular distributions such as ArchLinux, Debian, Fedora, and Red Hat Enterprise Linux.

CVE-2024-47176

- Found in the cups-browsed daemon (up to version 2.0.1), this vulnerability allows attackers to exploit the IPP protocol via UDP port 631 to manipulate printer configurations with malicious URLs.

CVE-2024-47076

- Present in libcupsfilters (up to version 2.1b1), this flaw lets attackers inject malicious data into other CUPS components.

CVE-2024-47175

- Affects libppd (up to version 2.1b1), allowing attackers to craft harmful data within temporary PPD files, leading to further system compromise.

CVE-2024-47177

- Targets cups-filters (up to version 2.0.1), allowing for arbitrary command execution via the FoomaticRIPCommandLine PPD parameter.

Affected Products:

- Operating Systems - Linux (ArchLinux, Debian, Fedora, RHEL, etc.), Unix-based systems (FreeBSD, OpenBSD, macOS)
- CUPS Versions - Versions up to 2.0.1 for cups-browsed, up to 2.1b1 for libcupsfilters and libppd

By chaining these vulnerabilities, attackers can replace or install new printers with malicious URLs, triggering remote code execution when a print job is initiated. Hundreds of thousands of devices were found to be potentially vulnerable. There have been no confirmed reports of attackers exploiting the vulnerabilities, but a proof-of-concept (PoC) is publicly available. Aspire recommends applying patches and workarounds as they become available.

Aspire Protects

- **Apply Patches** - Monitor vendor advisories for patch releases. OpenPrinting has issued fixes for CVE-2024-47175 and CVE-2024-47076, and a temporary workaround for CVE-2024-47176. Linux distributions are still working on porting fixes. Continue to check OpenPrinting's advisory for updates.
- Red Hat released guidance on how their customers can check whether cups-browsed is running on their system.
- While waiting for CUPS packages, please apply the recommendations below:
    - **Restrict UDP Port 631** - Block all traffic to UDP port 631 and consider restricting DNS-SD traffic to prevent exploitation.
    - **Disable cups-browsed** - If not required, disable the cups-browsed service or remove it entirely.

IoCs

There are no known IoCs associated with the above vulnerabilities at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

TTPs to Watch

- **Tactic: Initial Access (TA0001)**
    - Exploitation for Client Execution (T1203) – Attackers may leverage vulnerabilities in CUPS to gain initial access by tricking users into starting a print job, which then triggers malicious code execution.
- **Tactic: Execution (TA0002)**
    - Command and Scripting Interpreter (T1059) – Attackers may exploit the CUPS vulnerabilities to inject and execute malicious commands via the FoomaticRIPCommandLine PPD parameter.
- **Tactic: Execution (TA0002)**
    - Command and Scripting Interpreter (T1059) – Attackers may exploit the CUPS vulnerabilities to inject and execute malicious commands via the FoomaticRIPCommandLine PPD parameter.
- **Tactic: Execution (TA0002)**
    - Command and Scripting Interpreter (T1059) – Attackers may exploit the CUPS vulnerabilities to inject and execute malicious commands via the FoomaticRIPCommandLine PPD parameter.

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors. Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyberattacks.
- **Aspire Managed Security Services**
  - Aspire Managed Security Services provide remote security monitoring and device management – 24 hours a day, 7 days a week. By aggregating and correlating security events from across your IT environment, our remote security monitoring service eliminates "noise" and make sense of what really matters.
  - Our managed security portfolio includes:
    - Managed Firewall
    - Managed IDS/IPS
    - Security event monitoring & incident management
    - Managed Cisco ISE (Identity Services Engine)
    - Endpoint Protection

Supporting Documentation

oss-sec: Re: CUPS printing system vulnerabilities (seclists.org)

Attacking UNIX Systems via CUPS, Part I (evilsocket.net)

RHSB-2024-002 - OpenPrinting cups-filters | Red Hat Customer Portal