مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in OpenPrinting CUPS

Tracking #:432316341

Date:30-09-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed critical vulnerabilities in OpenPrinting CUPS that could be exploited to enable remote code execution, potentially resulting in data theft, system compromise, or denial of service on affected systems.

TECHNICAL DETAILS:

Critical vulnerabilities in Common Unix Printing System (CUPS), a widely used print server on Linux distributions and other platforms like BSDs (FreeBSD, NetBSD, OpenBSD), Oracle Solaris, and Google Chrome OS. These vulnerabilities, if exploited, could allow attackers to gain remote code execution on affected systems, potentially leading to data theft or system damage.

Severity: Critical

Vulnerability Details

- **CVE-2024-47176:** Affects cups-browsed <= 2.0.1. Allows attackers to send malicious IPP requests to trigger arbitrary command execution.
- **CVE-2024-47076:** Affects libcupsfilters <= 2.1b1. Allows attackers to inject malicious data into the CUPS system.
- **CVE-2024-47175:** Affects libppd <= 2.1b1. Allows attackers to inject malicious data into PPD files.
- **CVE-2024-47177:** Affects cups-filters <= 2.0.1. Allows attackers to execute arbitrary commands via the FoomaticRIPCommandLine PPD parameter.

Exploitation:
Attackers can exploit these vulnerabilities by:

1. **Enabling the** cups-browsed **service:** This service must be running for the attack to succeed.
2. **Advertising a malicious printer:** The attacker can advertise a malicious printer on a network accessible to vulnerable systems.
3. **Tricking a user into printing:** If a user attempts to print to the malicious printer, they could be exploited.

Remote, Unauthenticated Exploitation: Attackers can exploit these vulnerabilities from the public internet or within a network segment if UDP port 631 is exposed.

Detection:
To check if system is vulnerable, run the following command:

Bash
```
sudo systemctl status cups-browsed
```

If the service is running and the `BrowseRemoteProtocols` directive in `/etc/cups/cups-browsed.conf` is set to `cups`, the system is vulnerable.

Mitigation:
Disable the cups-browsed **service:**
Bash
```
sudo systemctl stop cups-browsed
sudo systemctl disable cups-browsed
```

Block UDP port 631: While this may not completely prevent exploitation on a LAN, it can help reduce the attack surface.

RECOMMENDATIONS:

- Implement mitigation measures until the patch is released.
- Apply the patches to address these vulnerabilities as soon as they are released.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.redhat.com/en/blog/red-hat-response-openprinting-cups-vulnerabilities
- https://www.rapid7.com/blog/post/2024/09/26/etr-multiple-vulnerabilities-in-common-unix-printing-system-cups/