مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Multiple Vulnerabilities in OpenPrinting CUPS

Tracking #:432317706

Date:15-09-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in OpenPrinting CUPS that could be exploited to carry out denial-of-service (DoS) attacks and gain unauthorized access to affected systems.

TECHNICAL DETAILS:

OpenPrinting has released security updates addressing two significant flaws in the Common Unix Printing System (CUPS), a widely used open-source printing service on Linux and Unix-like systems. These vulnerabilities, tracked as CVE-2025-58364 and CVE-2025-58060, can be exploited to trigger a remote denial-of-service (DoS) condition and enable authentication bypass under specific configurations. Successful exploitation could disrupt enterprise, education, and government printing environments or allow unauthorized administrative access.

Vulnerability Details
CVE-2025-58364: Remote DoS via Null Dereference

- CVSS Score: 6.5 (Medium)
- Severity: Medium
- Description: A flaw in the libcups library stems from unsafe deserialization and validation of printer attributes. Attackers on the same subnet can craft malicious responses, leading to a null dereference when ipp_read_io() passes data into ippValidateAttributes().
- Impact:
    - Causes CUPS and cups-browsed to crash, disrupting services.
    - Local network attackers can cause repeated Denial-of-Service conditions.
    - Internet-exposed systems may be remotely attacked if older vulnerabilities are also present.

CVE-2025-58060: Authentication Bypass with AuthType Negotiate

- CVSS Score: 8.0 (High)
- Severity: High
- Description: Systems configured with any AuthType other than Basic do not properly enforce authentication when receiving a Basic authorization header. Password validation is bypassed, potentially granting unauthorized access.
- Impact:
    - Direct authentication bypass in CUPS environments.
    - Attackers can perform administrative actions on printers, queues, and jobs without valid credentials.
    - Significantly increases exposure when CUPS is exposed beyond trusted networks.

Affected Versions

- CVE-2025-58364: Affects CUPS < 2.4.12
- CVE-2025-58060: Affects CUPS < 2.4.13

Fixed Versions

- CUPS 2.4.14 or later.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Vendor.

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://github.com/OpenPrinting/cups/security/advisories/GHSA-7qx3-r744-6qv4
- https://github.com/OpenPrinting/cups/security/advisories/GHSA-4c68-qgrh-rmmq
- https://github.com/OpenPrinting/cups/releases/tag/v2.4.14