مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerabilities in Canon Printers

Tracking #:432317306

Date:26-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Canon has disclosed multiple critical out-of-bounds write (buffer overflow) vulnerabilities in its Office/Small Office Multifunction and Laser Printers that could allow remote attackers to execute arbitrary code or cause Denial-of-Service (DoS) conditions on affected devices.

TECHNICAL DETAILS:

Canon Inc. has disclosed multiple critical out-of-bounds write (buffer overflow) vulnerabilities in its Office/Small Office Multifunction and Laser Printers. These vulnerabilities—tracked as **CVE-2024-12647**, **CVE-2024-12648**, **CVE-2024-12649**, and **CVE-2025-2146**—could allow remote attackers to execute arbitrary code or cause Denial-of-Service (DoS) conditions on affected devices. These flaws carry a **CVSS v3 base score of 9.8**, indicating **critical severity** and **no user interaction required** for exploitation.

Devices directly connected to the Internet without firewall protection are especially vulnerable. Canon has issued firmware updates and recommended operational mitigations to secure the affected products.

Technical Details:

- **Vulnerability Class:** Out-of-Bounds Write (CWE-787)
- **CVSS v3 Base Score:** 9.8 (CRITICAL)
  Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- **Impact:** Remote Code Execution (RCE), Denial-of-Service (DoS)
- **Attack Vector:** Remote (via direct network access)
- **Exploitation Prerequisites:** None (no authentication or user interaction required)

Affected Canon Printer Models:

imageCLASS MF Series:

- MF455DW, MF453DW, MF452DW, MF451DW
- MF656CDW, MF654CDW, MF653CDW, MF652CW
- MF1238 II
- MF1643iF II, MF1643i II

imageCLASS LBP Series:

- LBP237DW, LBP236DW
- LBP632CDW, LBP633CDW
- LBP1238 II

Note: Canon has stated that additional models may be added as assessments continue.

RECOMMENDATIONS:

- Organizations should update the firmware on all affected Canon printer models to the latest version as provided by Canon.
- Avoid exposing printers directly to the Internet.

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.usa.canon.com/support/canon-product-advisories/service-notice-regarding-vulnerability-measure-against-buffer-overflow-for-laser-printers-and-small-office-multifunctional-printers