



BUFFER OVERFLOW VULNERABILITIES IN CANON LASER PRINTERS AND MULTIFUNCTIONAL DEVICES

Vairav Advisory Report

Date: January 31, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

EXECUTIVE SUMMARY

Multiple buffer overflow vulnerabilities, identified as CVE-2024-12647, CVE-2024-12648, and CVE-2024-12649, have been discovered in Canon Laser Printers and Small Office Multifunctional Printers. These vulnerabilities could allow a remote attacker to execute arbitrary code or trigger a Denial-of-Service (DoS) condition if exploited. Devices directly connected to the Internet without a firewall or router are particularly vulnerable. Canon has advised users to update their firmware and implement network security measures to mitigate these risks.

VULNERABILITY DETAILS

CVE-2024-12647

Description: A buffer overflow in CPCA font download processing may allow an attacker on the same network segment to trigger a denial-of-service (DoS) condition or execute arbitrary code on the affected device.

Impact: Service disruption and potential unauthorized code execution.

CVSS Score: 9.8 (Critical)

CVE-2024-12648

Description: A buffer overflow in TIFF data EXIF tag processing may allow an attacker on the same network segment to cause the affected device to become unresponsive or execute arbitrary code.

Impact: Potential system takeover, unauthorized access, and denial of service.

CVSS Score: 9.8 (Critical)

CVE-2024-12649

Description: A buffer overflow in XPS data font processing that may allow an attacker on the same network segment to render the affected product unresponsive or execute arbitrary code.

Impact: Service disruption and potential unauthorized code execution.

CVSS Score: 9.8 (Critical)

AFFECTED VERSIONS

- imageCLASS MF Series: MF656CDW, MF654CDW, MF653CDW, MF652CW
- imageCLASS LBP Series: LBP632CDW, LBP633CDW

EXPLOIT DETAILS

These vulnerabilities can be exploited if a device is exposed to the Internet without proper security measures. Attackers could send specially crafted network packets to overflow the memory buffer, leading to arbitrary code execution or service disruptions.

RECOMMENDED ACTIONS

Patch & Upgrade:

Canon has released firmware updates to address these vulnerabilities. Users should immediately update their devices by following these steps:

- Touch Panel Model: Navigate to [Update Firmware] on the home screen, accept the license agreement, and proceed with the update.
- Black and White LCD Model: Access [Menu] > [Management Settings] > [Remote UI Settings/Update Firmware] > [Update Firmware] > [Via Internet]. Follow the on-screen instructions to complete the update.

ADDITIONAL SECURITY MEASURES

- Set the device's private IP address and restrict external access using a firewall, wired router, or Wi-Fi router.
- Enable logging features to detect potential exploitation attempts.
- Perform periodic reviews of device security settings and network configuration

REFERENCES

<https://www.cve.org/CVERecord?id=CVE-2024-12649>

<https://www.cve.org/CVERecord?id=CVE-2024-12648>

<https://www.cve.org/CVERecord?id=CVE-2024-12647>

<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>

<https://canon.jp/support/support-info/250127vulnerability-response>

<https://securityonline.info/cve-2024-12647-cvss-9-8-canon-printers-at-risk-of-remote-code-execution/>

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

Website: <https://vairavtech.com>