CVE-2025-1268: OUT-OF-BOUNDS VULNERABILITY IN PRINTER DRIVERS

Vairav CVE Report

Date: March 31, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Thirbam Sadak 148
Baluwatar, Kathmandu

EXECUTIVE SUMMARY

This report highlights a critical out-of-bounds vulnerability (CVE-2025-1268) discovered in certain Canon printer drivers for production printers, office/small office multifunction printers, and laser printers. The vulnerability can lead to arbitrary code execution when a malicious application processes a print job. Given its high severity, organizations should immediately update affected drivers to mitigate potential security risks.

VULNERABILITY DETAILS

CVE-2025-1268: Out-of-Bounds Vulnerability in Printer Drivers

Description: An out-of-bounds vulnerability exists in certain Canon printer drivers' Enhanced Metafile (EMF) Recode processing. This flaw can be exploited by a malicious application to disrupt printing or execute arbitrary code on the affected system.

Impact: Arbitrary code execution, system integrity compromise, and privilege escalation.

CVSS Score: 9.4 (Critical)

AFFECTED VERSIONS

- Generic Plus PCL6 Printer Driver – V3.12 and earlier
- Generic Plus UFR II Printer Driver – V3.12 and earlier
- Generic Plus LIPS4 Printer Driver – V3.12 and earlier
- Generic Plus LIPSLX Printer Driver – V3.12 and earlier
- Generic Plus PS Printer Driver – V3.12 and earlier

EXPLOIT DETAILS

Attackers can craft malicious print jobs that exploit the vulnerability to execute arbitrary code. Exploitation requires no user interaction and can be triggered remotely if the vulnerable driver is exposed via network printing.

RECOMMENDATIONS

- Download and install the latest fixed versions of printer drivers from the official Canon website or local Canon sales representatives.
- Restrict network access to printers to prevent unauthorized exploitation.

- Implement endpoint security measures to detect and block malicious print jobs.
- Regularly review and update security policies for networked printers.
- Monitor logs for any anomalous printing activity that may indicate exploitation attempts.

REFERENCES

https://securityonline.info/canon-fixes-critical-printer-driver-flaw-cve-2025-1268-alert/

https://psirt.canon/advisory-information/cp2025-003/

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: sales@vairavtech.com

Website: https://vairavtech.com