مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical RCE Vulnerability in Ricoh MFP and Printer Products

Tracking #:432316469

Date:05-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability has been discovered in Ricoh's Web Image Monitor, affecting numerous printer and MFP products.

TECHNICAL DETAILS:

Vulnerability Details:

- CVE ID: CVE-2024-47939
- CVSS Score: 9.8 (Critical)
- Affected Component: Web Image Monitor in Ricoh laser printers and MFPs
- Vulnerability Type: Stack-based buffer overflow (CWE-121)
- Potential Impact: Remote code execution, denial-of-service
- Exploitation Complexity: Low (no authentication required)
- A wide range of Ricoh laser printers and MFPs that implement Web Image Monitor are affected. For a complete list of vulnerable devices and corresponding firmware updates, refer to the official Ricoh security advisories

RECOMMENDATIONS:

- Identify all Ricoh printers and MFPs in the network that implement Web Image Monitor.
- Check Ricoh's official security advisories for a list of affected devices and corresponding firmware updates.
- Apply the latest firmware updates provided by Ricoh as soon as possible.

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.ricoh.com/products/security/vulnerabilities/vul?id=ricoh-2024-000011