مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Multiple Vulnerabilities in Brother Devices

Tracking #:432317429

Date:30-06-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed has security researchers has uncovered eight vulnerabilities in Brother Industries' multifunction printers (MFPs) and similar devices from FUJIFILM Business Innovation, Ricoh, Toshiba Tec Corporation, and Konica Minolta.

TECHNICAL DETAILS:

A recent investigation by Rapid7 has uncovered eight vulnerabilities in Brother Industries' multifunction printers (MFPs) and similar devices from FUJIFILM Business Innovation, Ricoh, Toshiba Tec Corporation, and Konica Minolta. The vulnerabilities affect a total of 748 printer, scanner, and label maker models, exposing users to risks such as unauthenticated remote access, remote code execution (RCE), denial of service (DoS), information leakage, and credential disclosure.

The most severe issue, CVE-2024-51978, is an authentication bypass vulnerability allowing attackers to derive the default administrator password from a leaked device serial number. 695 models are affected by this critical flaw, and due to its linkage to hardware-level password generation, firmware fixes are not sufficient. Brother has implemented a manufacturing process change and published workarounds for previously released models.

Firmware updates have been issued for seven of the eight vulnerabilities, while CVE-2024-51978 requires administrative action to mitigate. Enterprises using Brother or other impacted MFPs must take immediate steps to update firmware and secure device access

Vulnerability Details:

CVE ID	Description	Severity (CVSS)
CVE-2024-51977	Unauthenticated attacker can leak sensitive device information (e.g., serial number).	5.3 (Medium)
CVE-2024-51978	Authentication bypass – attacker can generate default admin password from leaked serial number.	9.8 (Critical)
CVE-2024-51979	Authenticated attacker can trigger stack-based buffer overflow – potential for RCE.	7.2 (High)
CVE-2024-51980	Unauthenticated attacker can force device to open a TCP connection (SSRF).	5.3 (Medium)
CVE-2024-51981	Unauthenticated attacker can force device to perform arbitrary HTTP requests (SSRF).	5.3 (Medium)
CVE-2024-51982	Unauthenticated attacker can crash device (DoS).	7.5 (High)
CVE-2024-51983	Unauthenticated attacker can crash device (DoS).	7.5 (High)

CVE-2024-51984	Authenticated attacker can disclose stored external service credentials.	6.8 (Medium)

Affected Vendors & Model Impact

- Brother – 689 affected models (printers, scanners, label makers)
- FUJIFILM Business Innovation – 46 models
- Ricoh – 5 models
- Toshiba Tec Corporation – 2 models
- Konica Minolta, Inc. – 6 models

A complete list of affected models is available via the CVE entries and vendor advisories.

Impact Analysis

- CVE-2024-51978 can be chained with CVE-2024-51977 to leak the device serial number and calculate the admin password, resulting in unauthenticated full administrative access.
- Combining CVE-2024-51978 + CVE-2024-51979 can lead to unauthenticated remote code execution (RCE).
- DoS vulnerabilities allow attackers to crash devices, impacting availability and business continuity.
- Credential leaks (CVE-2024-51984) expose organizations to lateral movement and data exfiltration risks.

RECOMMENDATIONS:

- Apply firmware updates provided by Brother and associated vendors to address vulnerabilities.
- Change the default administrator password immediately for all devices.
- For legacy models, apply the vendor-recommended workaround if firmware cannot fully address the flaw.
- Restrict access to device management interfaces to internal networks or VPN-only environments.

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.rapid7.com/blog/post/multiple-brother-devices-multiple-vulnerabilities-fixed/