Brother Printer Default Admin Password Vulnerability Exposes Hundreds of Models

TL;DR

Attackers can remotely generate default administrator passwords for 689 Brother printer models, and additional models from Fujifilm, Toshiba, Ricoh, and Konica Minolta, via critical vulnerability CVE-2024-51978 (CVSS 9.8). This vulnerability cannot be fully patched on existing devices through firmware.

*Attackers gaining admin access can compromise printers and execute malicious code. Organizations must **immediately change default passwords** and apply available firmware updates.*

Overview

Rapid7 discovered a critical vulnerability (CVE-2024-51978) impacting hundreds of Brother printer models, as well as select models from Fujifilm, Toshiba, Ricoh, and Konica Minolta. The flaw is in the default password generation algorithm used during manufacturing, where device serial numbers are predictably hashed into default admin passwords. Attackers can remotely retrieve these serial numbers via publicly accessible HTTP, HTTPS, IPP, PJL, or SNMP services, allowing them to change passwords.

Affected Products

- Brother printer models (689 models across laser, inkjet, scanners, label makers)
- Fujifilm Business Innovation (46 models)
- Konica Minolta (6 models)
- Ricoh (5 models)
- Toshiba Tec Corporation (2 models)

Exploiting this vulnerability gives attackers administrative control of affected devices. Once authenticated, attackers can modify device configurations, access sensitive scanned documents, read stored credentials, and trigger additional vulnerabilities (CVE-2024-51979 and CVE-2024-51984 - for remote code execution). This elevates the risk of attackers pivoting into other internal network resources.

While firmware updates addressing related flaws have been issued, Brother stated that CVE-2024-51978 cannot be fully remediated through firmware on already-produced

devices. New manufacturing processes are being implemented, but all existing printers remain vulnerable unless default admin passwords are immediately changed.

Aspire Protects

- Change admin passwords from defaults to strong, unique passwords **immediately**.
- Install firmware updates provided by Brother, Fujifilm, Toshiba, Ricoh, and Konica Minolta.
- Restrict printer admin interfaces (HTTP/HTTPS/IPP) from external or unsecured internal network access.
- Regularly audit printer usage for unexpected admin logins, configuration changes, or suspicious activities.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – Attackers exploit public-facing HTTP/HTTPS/IPP printer interfaces to leak device serial numbers.

Credential Access

- Brute Force [T1110] – Attackers systematically reconstruct default admin passwords using leaked serial numbers.

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – Attackers leverage administrative access obtained via default credentials to perform additional attacks, including remote code execution.

IoCs

There are no known IoCs associated with the above vulnerabilities at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Organizations using affected multifunction printer devices in the following sectors are at risk:

- Education
- Healthcare
- Retail and eCommerce
- Government
- Finance
- Manufacturing
- Technology

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Multiple Brother Devices: Multiple Vulnerabilities (FIXED) - Rapid7 Blog

NVD - CVE-2024-51978

NVD - CVE-2024-51979

NVD - CVE-2024-51984

Addressing Security Vulnerabilities | Brother

REQ-9503 - Vuln. Disclosure White Paper