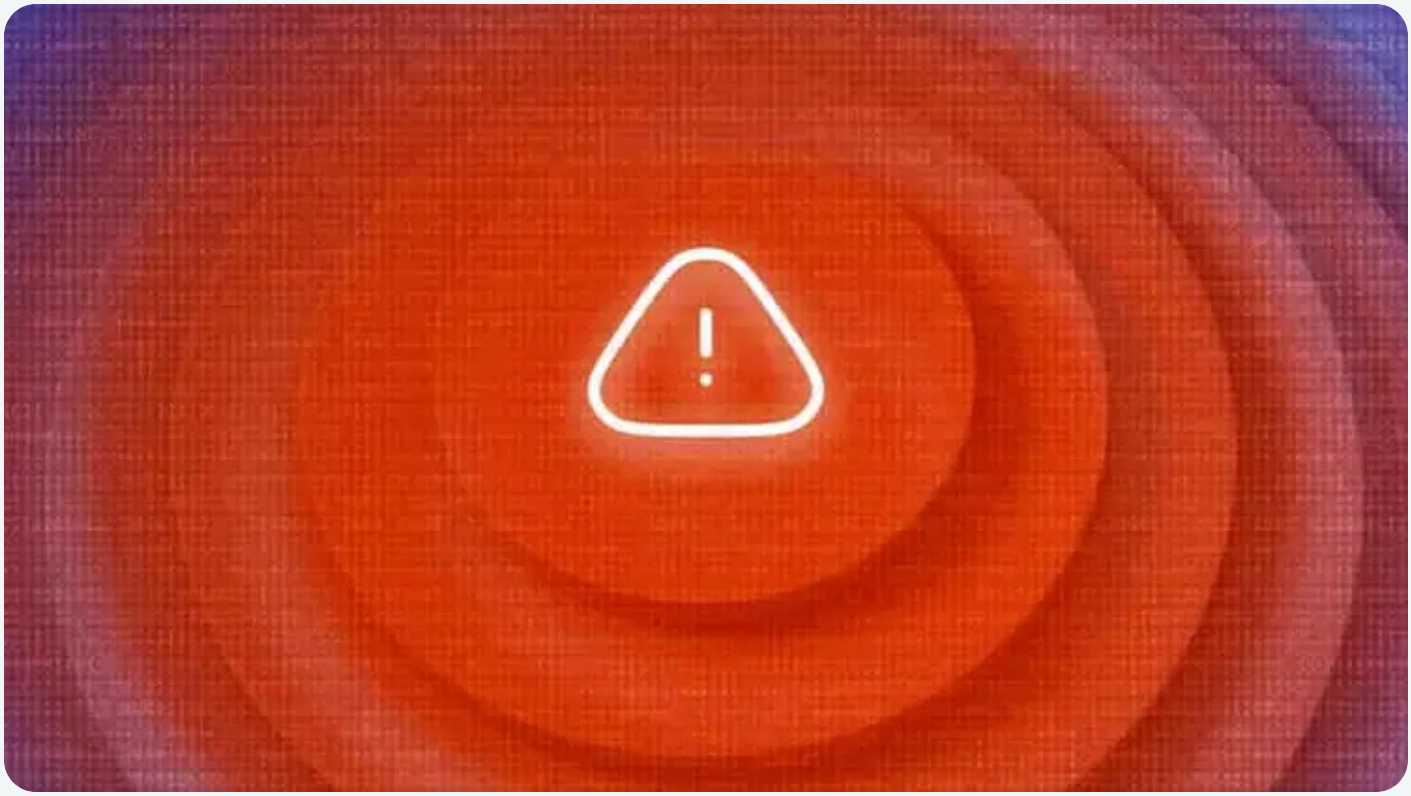
← BACK TO BLOG

VULNERABILITIES AND EXPLOITS

Multiple Brother Devices: Multiple Vulnerabilities (FIXED)

Stephen Fewer

Jun 25, 2025 | *Last updated on Sep 11, 2025* |



Overview

Update June 25, 2025: Update statistics to reflect an additional 6 affected models from Konica Minolta, Inc.

Rapid7 conducted a zero-day research project into multifunction printers (MFP) from Brother Industries, Ltd. This research resulted in the discovery of **8 new vulnerabilities**. Some or all of these vulnerabilities have been identified as affecting 689 models across Brother's range of printer, scanner, and label maker devices. Additionally, 46 printer models from FUJIFILM Business Innovation, 5 printer models from Ricoh, 2 printer models from Toshiba Tec Corporation, and 6 models from Konica Minolta, Inc. are affected by some or all of these vulnerabilities. In total, **748 models across 5 vendors are affected**. Rapid7, in conjunction with JPCERT/CC, has worked with Brother over the last thirteen months to coordinate the disclosure of these vulnerabilities.

The most serious of the findings is the **authentication bypass** CVE-2024-51978. A remote unauthenticated attacker can leak the target device's serial number through one of several means, and in turn generate the target device's default administrator password. This is due to the discovery of the default password generation procedure used by Brother devices. This procedure transforms a serial number into a default password. Affected devices have their default password set, based on each device's unique serial number, during the manufacturing process. **Brother has indicated that this vulnerability cannot be fully remediated in firmware, and has required a change to the manufacturing process of all affected models.** Only affected models that are made via this new manufacturing process will be fully remediated against CVE-2024-51978. For all affected models made via the old manufacturing process, Brother has provided a workaround.

A summary of the 8 vulnerabilities is shown below:

CVE	Description	Affected Service	CVSS
CVE-2024-51977	An unauthenticated attacker can leak sensitive information.	HTTP (Port 80), HTTPS (Port 443), IPP (Port 631)	5.3 (Medium)
CVE-2024-51978	An unauthenticated attacker can generate the	HTTP (Port 80), HTTPS (Port	9.8 (Critical)

CVE	Description	Affected Service	CVSS
	device's default administrator password.	443), IPP (Port 631)	
CVE-2024-51979	An authenticated attacker can trigger a stack based buffer overflow.	HTTP (Port 80), HTTPS (Port 443), IPP (Port 631)	7.2 (High)
CVE-2024-51980	An unauthenticated attacker can force the device to open a TCP connection.	Web Services over HTTP (Port 80)	5.3 (Medium)
CVE-2024-51981	An unauthenticated attacker can force the device to perform an arbitrary HTTP request.	Web Services over HTTP (Port 80)	5.3 (Medium)
CVE-2024-51982	An unauthenticated attacker can crash the device.	PJL (Port 9100)	7.5 (High)
CVE-2024-51983	An unauthenticated attacker can crash the device.	Web Services over HTTP (Port 80)	7.5 (High)
CVE-2024-51984	An authenticated attacker can disclose the password of a configured external service.	LDAP, FTP	6.8 (Medium)

Impact

The information leak vulnerability CVE-2024-51977 allows a remote unauthenticated attacker to leak the target device's serial number, along with several other pieces of

sensitive information. Knowing a target device's serial number is required to leverage the authentication bypass vulnerability CVE-2024-51978.

The authentication bypass vulnerability CVE-2024-51978 allows a remote unauthenticated attacker to generate the target device's default administrator password. The default password is generated during the manufacturing process by transforming the device's unique serial number into the default password. CVE-2024-51977 allows an attacker to leak a serial number via the target's HTTP, HTTPS, and IPP services. However, should an attacker not be able to leverage CVE-2024-51977, a remote unauthenticated attacker can still discover a target device's serial number via either a PJL or SNMP query. If the administrator password for the target device has not been changed, and therefore is still the default password, a remote unauthenticated attacker can use this default administrator password to either reconfigure the target device, or access functionality only intended for authenticated users.

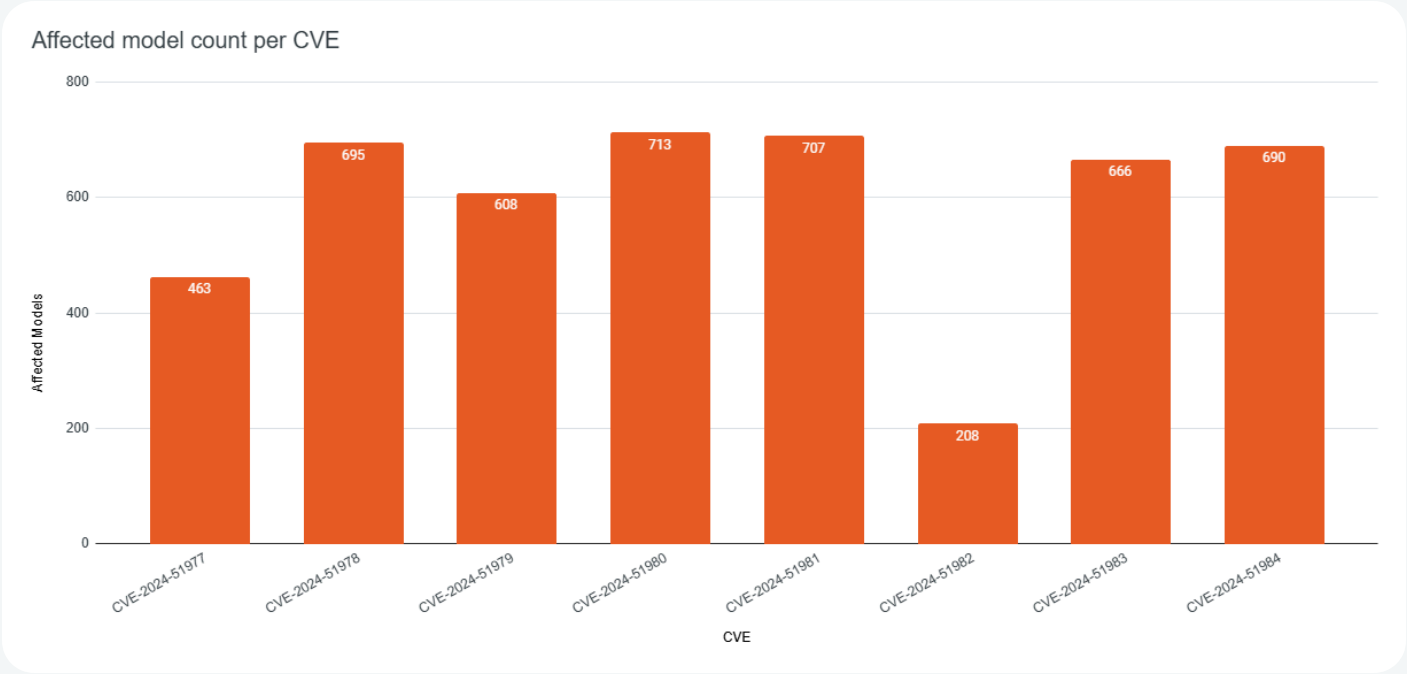
The vulnerability, CVE-2024-51979, allows an authenticated attacker to trigger a stack based buffer overflow vulnerability and in-turn control several CPU registers, including the Program Counter (PC). This is thought to be a sufficient exploit primitive for achieving remote code execution (RCE) on the target. In the context of a remote unauthenticated attacker who can successfully chain both the authentication bypass vulnerability CVE-2024-51978, and the stack based buffer overflow vulnerability CVE-2024-51979 together, the impact here will be unauthenticated RCE.

The 2 Server Side Request Forgery (SSRF) vulnerabilities, CVE-2024-51980, and CVE-2024-51981, allow an unauthenticated attacker to perform network connections via the target device. Depending on the attacker's position on the network, along with the target device's position on the network, this may allow a remote attacker on an external network to perform network connections via the target device located on an internal network, for example, when a printer's web interface is exposed across a network segment.

For the 2 denial of service (DoS) vulnerabilities, CVE-2024-51982 and CVE-2024-51983, an unauthenticated attacker with network access to a target device, can repeatedly crash a target device resulting in a complete loss of availability for the device.

The pass back vulnerability CVE-2024-51984, allows a remote authenticated attacker to discover the plaintext credentials of several configured external services, such as LDAP or FTP. Successfully exploiting this vulnerability gives an attacker additional credentials to use when trying to pivot further into a network environment. In the case of credentials to an external FTP service, these credentials may be used to disclose sensitive information such as documents stored on that FTP service.

Mapping the 8 vulnerabilities across the 748 affected models from the 5 vendors, we can see in the chart below the distribution of the number of affected models for each CVE. For example, 695 models are affected by the authentication bypass vulnerability CVE-2024-51978, while 208 models are affected by the denial of service vulnerability CVE-2024-51982.



Rapid7, acting as the CVE Numbering Authority (CNA) in this disclosure, has populated all 8 CVE records with information for every known affected model. Due to the amount of entries, this data will not be replicated in this disclosure blog post, and we recommend practitioners refer to the CVE records as the source of truth regarding affected models.

Technical analysis

A detailed technical analysis of the vulnerabilities described in this blog can be found in Rapid7's white paper "Print Scan Hacks: Identifying multiple vulnerabilities across multiple Brother devices".

The accompanying proof of concept source code for the white paper can be found here.

Credit

These vulnerabilities were discovered by Stephen Fewer, Principal Security Researcher at Rapid7 and are being disclosed in accordance with Rapid7's vulnerability disclosure policy.

Vendor statement

The following statement has been provided by Brother.

Brother would like to thank Rapid7 for their efforts in discovering the issues. We have informed our customers about the mitigation on our website.

Remediation

The following 7 vulnerabilities have been remediated via a firmware update available from the vendor:

- CVE-2024-51977
- CVE-2024-51979
- CVE-2024-51980
- CVE-2024-51981
- CVE-2024-51982
- CVE-2024-51983
- CVE-2024-51984

For the authentication bypass vulnerability CVE-2024-51978, the vendor has indicated that this vulnerability cannot be fully remediated in firmware, and instead has provided a workaround in their advisory.

Users of affected models should apply both the vendor supplied firmware updates and workarounds to remediate all 8 vulnerabilities. For additional details, please see the following vendor advisories:

- Brother Laser and Inkjet Printer Advisory
- Brother Document Scanner Advisory
- Brother Label Printer Advisory
- FUJIFILM Business Innovation Advisory
- Ricoh Advisory
- Toshiba Tec Corporation Advisory
- Konica Minolta, Inc. Advisory

Rapid7 customers

InsightVM and Nexpose customers will be able to assess exposure to CVE-2024-51977, CVE-2024-51978, CVE-2024-51982, and CVE-2024-51983 using unauthenticated checks expected to be available in the June 25 content release. The checks for CVE-2024-51982 and CVE-2024-51983 are designed to crash the system, hence customers have to opt in by having the “UNSAFE” check type enabled for checks to run successfully.

Disclosure timeline

- **May 3, 2024:** Rapid7 makes initial contact with Brother.
- **May 10, 2024:** Brother confirms receipt of disclosure document.
- **June 4, 2024:** Rapid7 provides additional clarity to several technical questions from Brother.
- **July 5, 2024:** Brother indicates all future communication will go through JPCERT/CC.
- **July 24, 2024:** JPCERT/CC make initial introductions and assign a case ID.
- **July 26, 2024:** JPCERT/CC provides a guide disclosure date of May 2025.
- **August 28, 2024:** JPCERT/CC affirms the disclosure schedule and gives June 2025 for the public disclosure.
- **October 10, 2024:** Rapid7 observes a firmware update for the MFC-L9570CDW contains fixes for several of the identified issues.
- **October 18, 2024:** Rapid7 contacts JPCERT/CC to seek clarification on the firmware release and the coordinated disclosure timeline.
- **November 1, 2024:** JPCERT/CC affirms the disclosure timeline for all affected models will remain as of June 2025.
- **November 5, 2024:** Rapid7 will act as the CNA and provide JPCERT/CC with 8 reserved CVE IDs.
- **November 19, 2024:** JPCERT/CC provides Rapid7 with a list of affected models.
- **March 5, 2025:** Brother requests Rapid7 to verify the fixes for 7 of the 8 vulnerabilities.
- **March 21, 2025:** Rapid7 verifies the fixes and provides Brother with a report detailing the results.
- **May 20, 2025:** Rapid7 requests an agreed upon date for a coordinated disclosure, and suggests June 25, 2025.
- **May 22, 2025:** JPCERT/CC confirms June 25, 2025 for a coordinated public disclosure.
- **June 2, 2025:** JPCERT/CC provides Rapid7 with an updated list of affected models.
- **June 20, 2025:** JPCERT/CC provides Rapid7 with URLs for upcoming vendor advisories.
- **June 25, 2025:** This disclosure.

- **June 25, 2025:** JPCERT/CC provides Rapid7 with details of six affected Konica Minolta, Inc models.

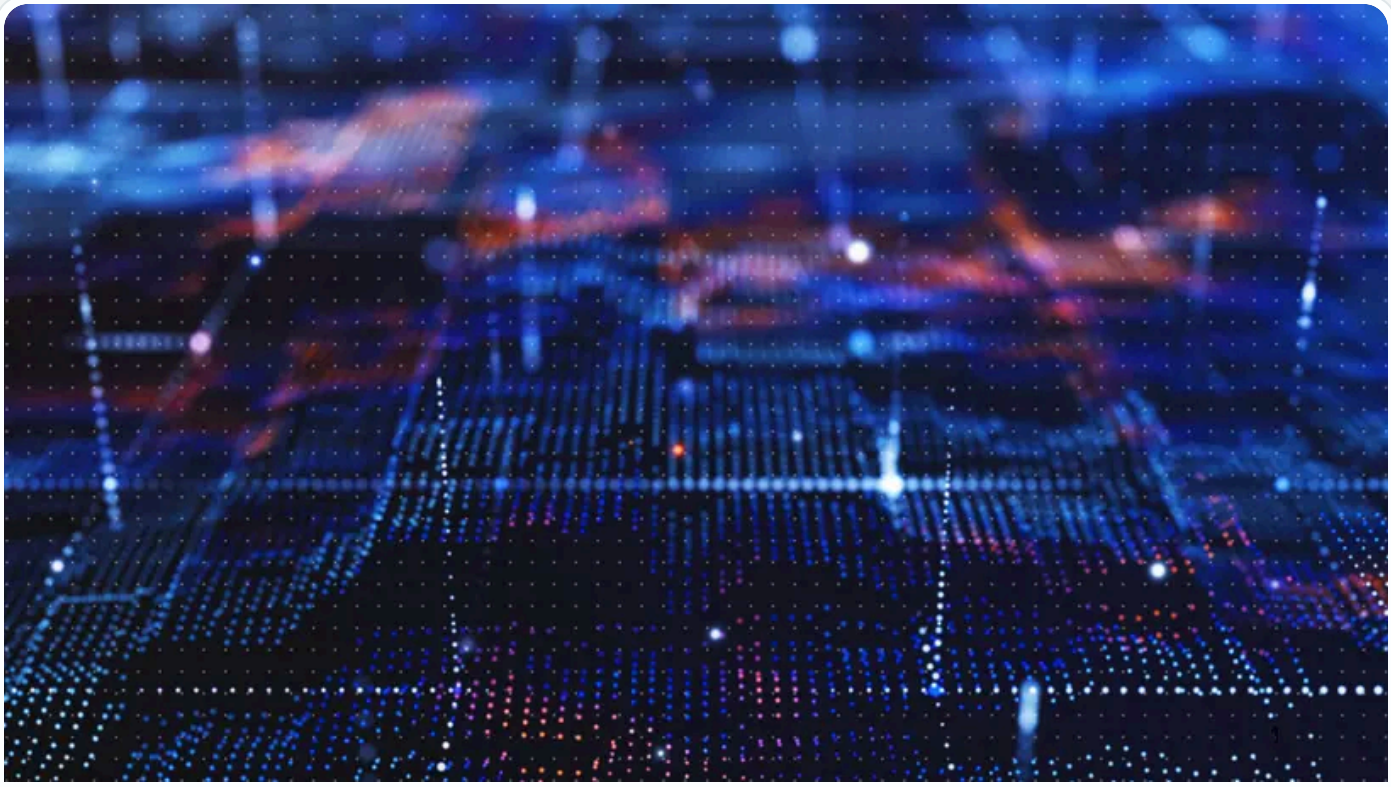
Article Tags

Research | Vulnerability Disclosure

Stephen Fewer

AUTHOR POSTS →

Related blog posts



THREAT RESEARCH

New Whitepaper: Stealthy BPFDoor Variants are a Needle That Looks Like Hay

Rapid7 Labs

THREAT RESEARCH

BPFdoor in Telecom Networks: Sleeper Cells in the Backbone

Rapid7 Labs

VULNERABILITIES AND EXPLOITS

CVE-2026-31381, CVE-2026-31382: Gainsight Assist Information Disclosure and Cross-Site Scripting (FIXED)

GET STARTED

Command Platform
Exposure Management
MDR Services

TAKE ACTION

Start a Free Trial
Take a Product Tour
Get Breach Support
Contact Sales

COMPANY

About Us

Leadership

Newsroom

Our Customers

Partner Programs

Investors

Careers

STAY INFORMED

Blog

Emergent Threat Response

Webinars & Events

Rapid7 Labs Research

Vulnerability Database

Security Fundamentals

FOR CUSTOMERS

Sign In

Support Portal

Product Documentation

Extension Library

Rapid7 Academy

Customer Escalation Portal

CONTACT SUPPORT

+1-866-390-8113

FOLLOW US

LinkedIn

X (Twitter)

Facebook

Instagram

Bluesky

© Rapid7

Legal Terms

Privacy Policy

Export Notice

Trust

Cookie List

Accessibility Statement