Multiple Brother Devices: Multiple Vulnerabilities

Overview

Rapid7 conducted a zero-day research project into multifunction printers (MFP) from Brother Industries, Ltd. This research resulted in the discovery of eight 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, 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.

A summary of the eight 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 device's default administrator password.	HTTP (Port 80), HTTPS (Port 443), IPP (Port 631)	9.8 (Critical)
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	Description	Affected Service	CVSS
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)

For more details on this disclosure, please read the Rapid7 disclosure blog post here.

Technical Analysis

A detailed technical analysis of these vulnerabilities can be found in Rapid7's white paper "Print Scan Hacks: Identifying multiple vulnerabilities across multiple Brother devices" (PDF).

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

Contributors 1

sfewer-r7 Stephen Fewer

Languages

- **Ruby** 100.0%