KONICA MINOLTA

Multiple vulnerabilities in B/W small multifunction and single-function printers

June 25, 2025
Konica Minolta, Inc.

Dear Customers,

We deeply appreciate your constant patronage to Konica Minolta products.
Multiple security vulnerabilities have been newly identified in the indicated models.
This advisory provides an overview of the issues and the recommended countermeasures.
Please note that, at the time of writing, there have been no confirmed security incidents globally resulting from the exploitation of these vulnerabilities.

Overview of the vulnerabilities

Ref. ID	Vulnerabilities description	Reference web site
CVE-2017-9765	Stack Buffer Overflow Vulnerability	https://www.cve.org/CVERecord?id=CVE-2017-9765
CVE-2024-2169	Infinite Loop of Messages Between Servers	https://www.cve.org/CVERecord?id=CVE-2024-2169
CVE-2024-51977	Possibility of information leakage in the printer	https://www.cve.org/CVERecord?id=CVE-2024-51977
CVE-2024-51978	Possibility of Authentication Bypass	https://www.cve.org/CVERecord?id=CVE-2024-51978
CVE-2024-51979	Possible Stack Overflow	https://www.cve.org/CVERecord?id=CVE-2024-51979
CVE-2024-51980	Possibility of a forced TCP connection	https://www.cve.org/CVERecord?id=CVE-2024-51980
CVE-2024-51981	Possibility of arbitrary HTTP request execution	https://www.cve.org/CVERecord?id=CVE-2024-51981
CVE-2024-51983	External attacks can cause device to crash	https://www.cve.org/CVERecord?id=CVE-2024-51983
CVE-2024-51984	Possibility of information leakage in the printer due to pass-back attacks	https://www.cve.org/CVERecord?id=CVE-2024-51984

Note: CVE-2024-51978 and CVE-2024-51979 have no impact on bizhub 3080MF/3000MF

KONICA MINOLTA

Affected Models and the countermeasure firmware

Product name	Program name	Affected version	Fixed version
bizhub 5020i	Main-Firmware	U2406280431（Ver R）or earlier	U2412241059 (Ver S）or later
	Sub-Firmware	1.13 or earlier	1.15 or later
bizhub 5000i	Main-Firmware	1.32 or earlier	1.33 or later
	Sub-Firmware	1.13 or earlier	1.15 or later
bizhub 4020i	Main-Firmware	U2406280431（Ver R）or earlier	U2412241059（Ver S）or later
	Sub-Firmware	1.13 or earlier	1.15 or later
bizhub 4000i	Main-Firmware	1.28 or earlier	1.29 or later
	Sub-Firmware	1.13 or earlier	1.15 or later
bizhub 3080MF	Controller firmware	N2403271808 or earlier	P2412101158 or later
bizhub 3000MF	Controller firmware	M2403271743 or earlier	N2412101132 or later

Remediation

- Download the Firmware Update Tool from Drivers & Downloads and upgrade the firmware of your device.
- If the default administrator password has not yet been changed, it is strongly recommended to update it to a complex and unique password immediately after the update.

Vulnerability Specific Recommendations

Ref. ID	Mitigations
CVE-2017-9765	Disable WSD feature.
CVE-2024-2169	Disable TFTP.
CVE-2024-51977	Upgrade to the latest firmware. (There is no workaround available.)
CVE-2024-51978	Change the administrator password from the default value.
CVE-2024-51979	Change the administrator password from the default value.

CVE-2024-51980	Disable WSD feature.
CVE-2024-51981	Disable WSD feature.
CVE-2024-51983	Disable WSD feature.
CVE-2024-51984	Disable WSD feature.

General Security Recommendations
To ensure a secure operating posture for your multifunction devices, and to reduce exposure to the vulnerabilities described in this advisory, Konica Minolta strongly recommends applying the following configuration best practices:

1. **Avoid Direct Internet Exposure**
   Place devices behind firewalls and use private IP addressing.

2. **Change Default Passwords**
   Change default credentials and implement strong passwords for administrative and network functions.

3. **Use Strong Passwords for Services**
   Ensure strong credentials are configured for SMTP, LDAP, and any other integrated services.

4. **Disable Unused Services**
   Turn off unused ports or protocols (specifically WSD & TFTP) to reduce attack surface.

5. **Use Secure Protocols**
   Configure devices to use encrypted communications (e.g., HTTPS, LDAPS, IPPS) where supported.

6. **Monitor Device Activity**
   Regularly review device logs and network traffic for suspicious behavior.

7. **Enable Authentication Where Available**
   Use built-in user authentication features to prevent unauthorized access to device functions.

Enhancing the Security of Products and Services
Konica Minolta considers the security of its products and services to be an important responsibility and will continue to actively respond to incidents and vulnerabilities.
https://www.konicaminolta.com/about/csr/social/customers/enhanced_security.html

Contact
Should you require further clarification or assistance with implementing the recommended measures or applying the relevant firmware update, please contact your authorized Konica Minolta service representative.