KONICA MINOLTA

Vulnerabilities in the CA certificate download and the diagnostic log functionality on B/W small multifunction and single-function printers

January 29, 2026
Konica Minolta, Inc.

Dear Customers,

We deeply appreciate your constant patronage to Konica Minolta products.
Two security vulnerabilities have been newly identified in the indicated models.
This advisory provides an overview of the issue and guidance on how to resolve them.
Please note that, at the time of publication, there have been no confirmed security incidents globally resulting from the exploitation of these vulnerabilities.

Overview of the vulnerabilities

CVE-ID	CVSS Assessment	Base Score	Vulnerabilities description
CVE-2025-53869	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N	6.3	The set of root certificates used by the product may be replaced with a set of arbitrary certificates by a man-in-the-middle attack. (CWE-295: Improper certificate validation)
	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N	3.7	
CVE-2025-55704	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N	6.9	An attacker may obtain the logs of the affected product and obtain sensitive information within the logs. (CWE-912: Hidden Functionality)
	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	5.3	

Affected Models

Product name	Program name	Affected version	Fixed version
bizhub 5021i	Firmware	1.02	1.04
bizhub 5001i	Firmware	1.03	1.05
bizhub 4221i	Firmware	1.02	1.04
bizhub 4201i	Firmware	1.02	1.04
bizhub 5020i	Main-Firmware	U2412241059 (Ver S) or earlier	U2505151336 (Ver T) or later
	Sub-Firmware	1.15 or earlier	1.16 or later
bizhub 5000i	Main-Firmware	1.33 or earlier	1.34 or later
	Sub-Firmware	1.15 or earlier	1.16 or later

bizhub 4020i	Main-Firmware	U2412241059 (Ver S) or earlier	U2505151336 (Ver T) or later
	Sub-Firmware	1.15 or earlier	1.16 or later
bizhub 4000i	Main-Firmware	1.29 or earlier	1.30 or later
	Sub-Firmware	1.15 or earlier	1.16 or later

Remediation
Download the Firmware Update Tool from Drivers & Downloads and upgrade the firmware of your device.

General Security Recommendations
To ensure a secure operating posture for your multifunction devices, and to reduce exposure to the vulnerability 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, SMB, WebDAV, and any other integrated services.

4. **Disable Unused Services**
   Turn off unused ports or protocols 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.

For comprehensive information on secure configuration, please refer to our Product Security web site.
https://www.konicaminolta.com/global-en/security/mfp/setting/index.html

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

Related Information
JVNVU#92878805

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.