KONICA MINOLTA

Security vulnerability (CVE-2025-8452) in B/W small multifunction and single-function printers

September 17, 2025
Konica Minolta, Inc.

Dear Customers,

We deeply appreciate your constant patronage to Konica Minolta products.
A new vulnerability (CVE-2025-8452) related to CVE-2024-51978, has been identified in connection with the security issue disclosed on June 25, 2025. This advisory provides an overview of the issue and the recommended remediation.
Please note that, at the time of publication, there have been no confirmed security incidents globally resulting from the exploitation of this vulnerability.

Overview of the vulnerability

Reference ID	CVSSv3.1	Base Score	EPSS*	Vulnerabilities description
CVE-2025-8452	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	4.3	0.02%	Through the use of eSCL or SNMP protocols, an attacker can retrieve the serial number of a printer. By applying the attack technique described in CVE-2024-51978, the default administrator password can be derived from the obtained serial number. Consequently, if the administrator password has not been changed from its default setting, there is a risk that an attacker could use the generated password to gain unauthorized control of the device.

*EPSS: Probability of exploitation activity in the next 30 days

Affected Models and Remediation

Product name	Affected version	Remediation
bizhub 5020i	All versions	Ensure that the administrator password is secure. If it remains set to its factory default, please change it immediately to a strong complex password. Configuration: 1. Enter the printer's IP address into the address bar of your computer's web browser. 2. On the login screen, enter the administrator password and click the right arrow button. 3. Navigate to the [Administrator] tab, then under [Login Password], enter [Enter Old Password], [Enter New Password], and [Confirm New Password]. Finally, click [OK] to apply the changes.
bizhub 5000i		
bizhub 4020i		
bizhub 4000i		

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#93294882

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.