KONICA MINOLTA

Pass-Back Attack Vulnerability in Konica Minolta Multifunction Printers

June 30, 2025
Konica Minolta, Inc.

Dear Customers,

We deeply appreciate your constant patronage to Konica Minolta products.
A Pass-Back Attack vulnerability has been newly identified in the indicated models.
This advisory provides an overview of the issue and the recommended countermeasures.
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

Ref. ID	CVSSv3.1 (Rapid7)	Base Score	Vulnerability description
CVE-2025-6081	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N	6.8	An authenticated attacker can disclose the password of a configured external service.

Affected Models

Product name	Affected version
bizhub C751i bizhub C651i/C551i/C451i bizhub C361i/C301i/C251i bizhub C4051i/C3351i/C4001i/C3301i bizhub C3321i bizhub 751i bizhub 651i/551i/451i bizhub 361i/301i bizhub 4751i/4051i bizhub 4701i bizhub C750i bizhub C650i/C550i/C450i bizhub C360i/C300i/C250i bizhub C287i/C257i/C227i bizhub C4050i/C3350i/C4000i/C3300i bizhub C3320i bizhub 950i/850i bizhub 750i bizhub 650i/550i/450i bizhub 360i/300i bizhub 306i/266i/246i/226i bizhub 4750i/4050i bizhub 4700i	All versions
bizhub C759/C659 bizhub C658/C558/C458 bizhub C368/C308/C258 bizhub C287/C227	All versions

bizhub C3851/C3851FS/C3351 bizhub 958/808/758 bizhub 658e/558e/458e bizhub 368e/308e bizhub 558/458/368/308 bizhub 367/287/227 bizhub 4752/4052	

Impact on Multifunction Printers
There is a possibility that authentication credentials configured for external services—such as LDAP, SMTP, FTP, SMB, or WebDAV—may be exposed by means of a malicious server connection.

Vulnerability Specific Recommendation
1. Ensure that the administrator password is secure. If it remains set to its factory default, please change it immediately to a strong complex password.
2. Restrict non-Admin users from making any address book destination changes.
3. When utilizing any external service, avoid registering accounts with elevated privileges—such as those used in systems like Active Directory—on the multifunction printers.

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 and Device IP Filtering settings.

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

Acknowledgements
We would like to express our sincere appreciation to Mr. Deral Heiland of Rapid7 and security researcher

Mr. Vladislav Volozhenko for discovering and responsibly reporting this vulnerability.

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.