



KONICA MINOLTA

Vulnerabilities affecting the Web Connection of Konica Minolta MFPs

Published: June 30, 2025
Last Updated: September 16, 2025
Konica Minolta, Inc.

Dear Customers,

We deeply appreciate your constant patronage to Konica Minolta products.

Two vulnerabilities have 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 these vulnerabilities.

Overview of the vulnerabilities

Ref. ID	CVSSv3.1	Base Score	EPSS*	Vulnerabilities description
CVE-2025-5884	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N	3.5	0.04%	Cross-site scripting vulnerability (CWE94, CWE-79) was found in the specific input fields of the Web Connection.
CVE-2025-5885	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N	4.3	0.02%	Cross-site request forgery vulnerability (CWE-352, CWE-862) was found in the Web Connection.

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

Affected Models and Countermeasure Firmware

Product name	Affected version	Fixed version
bizhub C759/C659 bizhub C658/C558/C458 bizhub C368/C308/C258 bizhub C287/C227 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	G00-YE or earlier	GG1-YE or later

Impact on Multifunction Printers

CVE-2025-5884:

An arbitrary script may be executed on the web browser of the user accessing the Web Connection.

CVE-2025-5885:

There is a possibility that the configuration of the device may be changed unintentionally, or that an unintended operation may be performed.

Remediation

The countermeasure firmware will be applied sequentially, either remotely or during the next visit by



KONICA MINOLTA

your authorized Konica Minolta service representative.

Vulnerability Specific Recommendation

If possible, completely disable the Web Connection. The vulnerability will not be exploitable as a result. Alternatively, kindly follow our general recommendations.

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

Related Information

<https://nvd.nist.gov/vuln/detail/CVE-2025-5884>

<https://nvd.nist.gov/vuln/detail/CVE-2025-5885>

Acknowledgements

We would like to express our sincere appreciation to the VulDB CNA Team 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.

Update history

Sep. 16, 2025: Added the countermeasure firmware information.