FAQs & Troubleshooting

Date: 07/09/2025 ID: faq00100848_000

Addressing Security Vulnerabilities

Description

A number of vulnerabilities that may affect Brother scanners have been identified and listed in the table below.

Vulnerability Identifier	Details and Reference URL
CVE-2017-9765	Stack buffer overflow that may allow malicious code execution or application crash https://www.cve.org/CVERecord?id=CVE-2017-9765
CVE-2024-2169	Infinite message loop between servers that may lead to denial of service https://www.cve.org/CVERecord?id=CVE-2024-2169
CVE-2024-51978	Authentication bypass risk https://www.cve.org/CVERecord?id=CVE-2024-51978
CVE-2024-51979	Risk of stack overflow that may lead to system instability and malicious code execution https://www.cve.org/CVERecord?id=CVE-2024-51979
CVE-2024-51980	Forced TCP connections that may lead to unauthorized remote access https://www.cve.org/CVERecord?id=CVE-2024-51980
CVE-2024-51981	Risk of unauthorized HTTP requests being forwarded to other hosts within the local area network https://www.cve.org/CVERecord?id=CVE-2024-51981
CVE-2024-51982	Device crash triggered by external input that may lead to denial of service and system instability https://www.cve.org/CVERecord?id=CVE-2024-51982
CVE-2024-51983	Risk of device crash from external input that may lead to denial of service and system instability https://www.cve.org/CVERecord?id=CVE-2024-51983
CVE-2024-51984	Risk of printer data exposure via pass-back attacks https://www.cve.org/CVERecord?id=CVE-2024-51984

View the list of affected scanners and firmware update status

Solution

To reduce the risks associated with the listed vulnerabilities, make sure you complete all three steps below:

1. Use the link above to check if an updated version of the affected firmware is available for your machine.
2. If an update is available, download and install the latest firmware version using the Firmware Update Tool.
3. After installation, change the default administrator password via Web Based Management.

If the updated firmware is not yet available:

- Follow the suggested workarounds in the “Workarounds” section.
- Regularly check the update availability status using the link above.
- Install the update as soon as it becomes available.
- Make sure you use your machine in a firewall-protected environment.

To maintain the highest level of security, we strongly recommend changing default passwords and regularly updating firmware.

Workarounds

As a temporary measure before the firmware update for your scanner becomes available, you can change the following settings from your scanner’s Web Based Management menu:

Vulnerability Identifier	Workaround
CVE-2017-9765	Disable the WSD function.

CVE-2024-2169	Disable TFTP.
CVE-2024-51978	Change the default administrator password.
CVE-2024-51979	Change the default administrator password.
CVE-2024-51980	Disable the WSD function.
CVE-2024-51981	Disable the WSD function.
CVE-2024-51982	There is no workaround. Install the latest firmware.
CVE-2024-51983	Disable the WSD function.
CVE-2024-51984	Change the default administrator password.

Acknowledgements
We would like to thank Yepeng Pan of CISPA, Germany, for reporting the CVE-2024-2169 vulnerability.
We would like to thank Stephen Fewer, Principal Security Researcher at Rapid7, USA, for reporting vulnerabilities CVE-2024-51977 - CVE-2024-51984.

If your question was not answered, have you checked other FAQs?

- Go to the Top page in the FAQs & Troubleshooting section
- See other FAQs in this category

Have you checked the manuals?

- Go to the Manuals section

Do you need any further assistance?

- Go to the Contact Us section

Content Feedback

To help us improve our support, please provide your feedback below.

Step 1: How does the information on this page help you?

- ○ Very helpful
- ○ Helpful
- ○ Not helpful

Step 2: Are there any comments you would like to add?

Please note this form is used for feedback only.

Clear Submit