



FUJIFILM Business Innovation

Important News

June 25, 2025

Dear Customers,

Thank you for your continued use of our products.

It has been discovered that some of our MFPs and printers have multiple vulnerabilities. The affected products are listed below.

We apologize for any inconvenience this may cause, but we ask that you please check if the model you are using is one of the affected models, and if so, please update the firmware.

At the time of publication of this notice, we have not confirmed any attacks using these vulnerabilities.

Vulnerability Description

We will mainly explain the impact of the above vulnerabilities. For the official names and technical details of the vulnerabilities, please refer to the CVE numbers in the "Related Information" section.

① Possibility of device hang (CVE-2017-9765)

If a maliciously modified message is received, the device may hang. No information stored on the device will be leaked. The device can be restored by turning it off and on again.

Cookieの利用について

「Cookieを受け入れる」をクリックすると、サイトナビゲーションを強化し、サイトの使用状況を分析し、弊社のマーケティング活動を支援するために、デバイスにCookieを保存することに同意したことになります。 [プライバシーポリシー](#)

[Cookie 設定](#)

[すべて拒否する](#)

[Cookie を受け入れる](#)

② Possibility of Mass Message Transmission Between Devices (CVE-2024-2169)

If a device receives a maliciously altered message, a chain reaction of message transmission may occur, increasing network load and potentially causing communication disruption and network service disruption (DoS).

③ Possibility of device configuration information being read (CVE-2024-51977)

Some device configuration information may be read through unauthorized access. Job content or address books will not be read.

④ Possibility of device hang-up (CVE-2024-51979)

If a device receives a maliciously modified message, it may hang up. No information stored on the device will be leaked. The device can be restored by turning the power off and then on again.

⑤ Possibility of port scanning (CVE-2024-51980)

It may be possible to perform port scanning on other devices within the same network using certain device functions.

⑥ Possibility of server-side request forgery attacks (CVE-2024-51981)

If a maliciously modified message is received, it may be possible to send a different message to other devices or terminals.

⑦ Possibility of device reboot (CVE-2024-51982)

Receiving maliciously crafted messages may cause the device to reboot.

Cookieの利用について

「Cookieを受け入れる」をクリックすると、サイトナビゲーションを強化し、サイトの使用状況を分析し、弊社のマーケティング活動を支援するために、デバイスにCookieを保存することに同意したことになります。[プライバシーポリシー](#) - 2024-51983

⑧ Possibility of device reboot (CVE-2024-51983)

Receiving maliciously crafted messages may cause the device to reboot.

⑨ Possibility of pass-back attack (CVE-2024-51984)

If an attacker has access to the device's configuration information, they may be able to perform a pass-back attack by modifying the destination of requests sent to external services registered on the device, thereby reading the credentials of those external services.

Affected Models

Product Name	Affected firmware version	Fixed firmware version	Vulnerability #								
			①	②	③	④	⑤	⑥	⑦	⑧	⑨
ApeosPrint 4620 SDN	Ver. 1.03	Ver. 1.04 or later	-	-	-	-	Y	-	-	-	-
ApeosPrint 4620 SDW	Ver. 1.03	Ver. 1.04 or later	-	-	-	-	Y	-	-	-	-
Apeos 4620 SDF	Ver. 1.03	Ver. 1.04 or later	-	-	-	-	Y	-	-	-	-
Apeos 4620 SZ	Ver. 1.03	Ver. 1.04 or later	-	-	-	-	Y	-	-	-	-
Apeos 4620 SX	Ver. 1.03	Ver. 1.04 or later	-	-	-	-	Y	-	-	-	-
DocuPrint P378 d	Ver.1.21 or earlier	Ver.1.24 or later	Y	Y	Y	Y	Y	Y	-	Y	Y
DocuPrint P375 d	Ver.1.21 or earlier	Ver.1.24 or later	Y	Y	Y	Y	Y	Y	-	Y	Y
DocuPrint P375 dw	Ver.1.21 or earlier	Ver.1.24 or later	Y	Y	Y	Y	Y	Y	-	Y	Y

Cookieの利用について

DocuPrint P375 dw 「Cookieを受け入れる」をクリックすると、サイトナビゲーションを強化し、サイトの使用状況を分析し、弊社のマーケティング活動を支援するために、デバイスにCookieを保存することに同意したことになります。 [プライバシーポリシー](#)

DocuPrint P385 dw	Ver.1.19 or earlier	Ver.1.22 or later	Y	Y	Y	Y	Y	Y	-	Y	Y
DocuPrint P388 dw	Ver.1.19 or earlier	Ver.1.22 or later	Y	Y	Y	Y	Y	Y	-	Y	Y
DocuPrint M378 d	Ver. K or earlier	Ver. L or later	Y	Y	Y	Y	Y	Y	-	Y	Y
DocuPrint M375 df	Ver. K or earlier	Ver. L or later	Y	Y	Y	Y	Y	Y	-	Y	Y
DocuPrint M378 df	Ver. K or earlier	Ver. L or later	Y	Y	Y	Y	Y	Y	-	Y	Y
DocuPrint M375 z	Ver. K or earlier	Ver. L or later	Y	Y	Y	Y	Y	Y	-	Y	Y
DocuPrint M385 z	Ver. L or earlier	Ver. M or later	Y	Y	Y	Y	Y	Y	-	Y	Y
DocuPrint P235 d	Ver.1.15 or earlier	Ver. 1.17 or later	Y	Y	Y	Y	Y	Y	Y	Y	Y
DocuPrint P275 dw	Ver.1.15 or earlier	Ver. 1.17 or later	Y	Y	Y	Y	Y	Y	Y	Y	Y
DocuPrint P285 dw	Ver.1.15 or earlier	Ver. 1.17 or later	Y	Y	Y	Y	Y	Y	Y	Y	Y
DocuPrint P288 dw	Ver.1.15 or earlier	Ver. 1.17 or later	Y	Y	Y	Y	Y	Y	Y	Y	Y
DocuPrint M235 dw	Ver. K or earlier	Ver. L or later	Y	Y	Y	Y	Y	Y	Y	Y	Y

Cookieの利用について

DocuPrint M235 z 「Cookieを受け入れる」をクリックすると、サイトナビゲーションを強化し、サイトの使用状況を分析し、弊社のマーケティング活動を支援するために、デバイスにCookieを保存することに同意したことになります。 [プライバシーポリシー](#)

DocuPrint M275z	Ver. L or earlier	Ver. M or later	Y	Y	Y	Y	Y	Y	Y	Y	Y
DocuPrint M285z	Ver. L or earlier	Ver. M or later	Y	Y	Y	Y	Y	Y	Y	Y	Y
DocuPrint M288dw	Ver. E or earlier	Ver. F or later	Y	Y	Y	Y	Y	Y	Y	Y	Y
DocuPrint M288z	Ver. E or earlier	Ver. F or later	Y	Y	Y	Y	Y	Y	Y	Y	Y
DocuPrint P225d	Ver.1.18 or earlier	Ver.1.20 or later	Y	Y	Y	-	Y	Y	-	Y	Y
DocuPrint P268d	Ver.1.22 or earlier	Ver.1.24 or later	Y	Y	Y	-	Y	Y	-	Y	Y
DocuPrint P268dw	Ver.1.22 or earlier	Ver.1.24 or later	Y	Y	Y	-	Y	Y	-	Y	Y
DocuPrint P265dw	Ver.1.22 or earlier	Ver.1.24 or later	Y	Y	Y	-	Y	Y	-	Y	Y
DocuPrint M268dw	Ver.M or earlier	Ver. N or later	Y	Y	Y	-	Y	Y	-	Y	Y
DocuPrint M268z	Ver.M or earlier	Ver. N or later	Y	Y	Y	-	Y	Y	-	Y	Y
DocuPrint M225dw	Ver.P or earlier	Ver. Q or later	Y	Y	Y	-	Y	Y	-	Y	Y
DocuPrint M225z	Ver.P or earlier	Ver. Q or later	Y	Y	Y	-	Y	Y	-	Y	Y

Cookieの利用について

DocuPrint M225z 「Cookieを受け入れる」をクリックすると、サイトナビゲーションを強化し、サイトの使用状況を分析し、弊社のマーケティング活動を支援するために、デバイスにCookieを保存することに同意したことになります。 [プライバシーポリシー](#)

Y	-	Y	Y	-	Y	Y
---	---	---	---	---	---	---

DocuPrint P118w	Ver. 1.12 or earlier	Ver. 1.14 or later	Y	Y	Y	-	Y	Y	-	Y	Y
DocuPrint P115w	Ver. 1.12 or earlier	Ver. 1.14 or later	Y	Y	Y	-	Y	Y	-	Y	Y
DocuPrint M118w	Ver. M or earlier	Ver. N or later	Y	Y	Y	-	Y	Y	-	Y	Y
DocuPrint M118z	Ver. M or earlier	Ver. N or later	Y	Y	Y	-	Y	Y	-	Y	Y
DocuPrint M115w	Ver. M or earlier	Ver. N or later	Y	Y	Y	-	Y	Y	-	Y	Y
DocuPrint M115fw	Ver. M or earlier	Ver. N or later	Y	Y	Y	-	Y	Y	-	Y	Y
DocuPrint M115z	Ver. M or earlier	Ver. N or later	Y	Y	Y	-	Y	Y	-	Y	Y

Y: affected, -: not affected

The models affected by this vulnerability are only those listed above.

For details on each vulnerability, please refer to the "Vulnerability Details" section above.

Countermeasure

Please apply the firmware that fixes this vulnerability.

Workaround


Cookieの利用について


「Cookieを受け入れる」をクリックすると、サイトナビゲーションを強化し、サイトの使用状況を分析し、弊社のマーケティング活動を支援するために、デバイスにCookieを保存することに同意したことになります。 [プライバシーポリシー](#)


Please take the following workarounds to apply the firmware version that fixes this vulnerability is applied. The following workarounds will reduce the risk of attacks caused by these vulnerabilities.


- Use the device within a network protected by a firewall, etc.
- When allowing access from the Internet, consider allowing access only to necessary IP addresses or using a VPN connection.


Related Information


[CVE-2017-9765](#) 


[CVE-2024-2169](#) 


[CVE-2024-51977](#) 


[CVE-2024-51979](#) 

[CVE-2024-51980](#) 

[CVE-2024-51981](#) 


[CVE-2024-51982](#) 

[CVE-2024-51983](#) 

[CVE-2024-51984](#) 

Contact

Please visit FUJIFILM Business Innovation support website to find for more details:

<https://support-fb.fujifilm.com/> 

Back to List



Cookieの利用について

「Cookieを受け入れる」をクリックすると、サイトナビゲーションを強化し、サイトの使用状況を分析し、弊社のマーケティング活動を支援するために、デバイスにCookieを保存することに同意したことになります。 [プライバシーポリシー](#)

©FUJIFILM Business Innovation Corp. / FUJIFILM Business Innovation Japan Corp.

Cookieの利用について

「Cookieを受け入れる」をクリックすると、サイトナビゲーションを強化し、サイトの使用状況を分析し、弊社のマーケティング活動を支援するために、デバイスにCookieを保存することに同意したことになります。 [プライバシーポリシー](#)