



[Home](#) > [Sustainability](#) > [Governance](#) > [Information Security](#) > [Product security](#) > [Information List by Vulnerability](#) > Vulnerability Information

# Specific Ricoh MFP and Printer Products - Multiple vulnerabilities (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)

First published: 07:00 am on June 25, 2025 (2025-06-25T16:00:00+09:00)  
Ricoh Company, Ltd.

Ricoh has identified Vulnerability : ricoh-2025-000007

This website uses cookies and other tracking technologies to enhance user experience and to analyze performance and traffic on our website. We also share information about your use of our site with our social media, advertising and analytics partners. If we have detected an opt-out preference signal then it will be honored. Further information is available in our [Cookie Policy](#).

Rejecting cookies may impact your experience on the website, such as playing YouTube videos. [Cookie Policy](#)

Do Not Sell or Share My Personal Information

Accept All Cookies



software).

These vulnerabilities are listed below along with their corresponding CVE identifiers:

CVE-2024-51981 ( [CWE-516](#), [CWE-93](#) )

CVE-2024-51982 ( [CWE-1286](#) )

CVE-2024-51983 ( [CWE-1286](#) )

CVE-2024-51984 ( [CWE-522](#) )

CVSSv3 base score : 8.1 **HIGH**

CVE-2017-9765: Stack buffer overflow that may allow malicious code execution or application crash

> <https://www.cve.org/CVERRecord?id=CVE-2017-9765>

CVE-2024-2169: Infinite message loop between servers that may lead to denial of service

> <https://www.cve.org/CVERRecord?>

This website uses cookies and other tracking technologies to enhance user experience and to analyze performance and traffic on our website. We also share information about your use of our site with our social media, advertising and analytics partners. If we have detected an opt-out preference signal then it will be honored. Further information is available in our [Cookie Policy](#).

Rejecting cookies may impact your experience on the website, such as playing YouTube videos. [Cookie Policy](#)

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 unauthorised remote access

> <https://www.cve.org/CVERecord?id=CVE-2024-51980>

CVE-2024-

51981: Risk of unauthorised HTTP requests being forwarded to other hosts within the local area network

This website uses cookies and other tracking technologies to enhance user experience and to analyze performance and traffic on our website. We also share information about your use of our site with our social media, advertising and analytics partners. If we have detected an opt-out preference signal then it will be honored. Further information is available in our [Cookie Policy](#).

Rejecting cookies may impact your experience on the website, such as playing YouTube videos. [Cookie Policy](#)

of service and

system

instability

> [https://www.cve.org/CVERecord?  
id=CVE-2024-51982](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](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](https://www.cve.org/CVERecord?id=CVE-2024-51984)

List 1 below

shows the

affected

products and

services.

This website uses cookies and other tracking technologies to enhance user experience and to analyze performance and traffic on our website. We also share information about your use of our site with our social media, advertising and analytics partners. If we have detected an opt-out preference signal then it will be honored. Further information is available in our [Cookie Policy](#).

Rejecting cookies may impact your experience on the website, such as playing YouTube videos. [Cookie Policy](#)

## List1:Ricoh products and services affected by this vulnerability

Product/service	Link to details
SP 230DNw	Affected. For details, please refer to the following URL. > <a href="https://www.ricoh.com/products/security/vulnerabilities/adv?id=ricoh-prod000166-2025-000007">https://www.ricoh.com/products/security/vulnerabilities/adv?id=ricoh-prod000166-2025-000007</a>
P 201W	Affected. For details, please refer to the following URL. > <a href="https://www.ricoh.com/products/security/vulnerabilities/adv?id=ricoh-prod000167-2025-000007">https://www.ricoh.com/products/security/vulnerabilities/adv?id=ricoh-prod000167-2025-000007</a>
M 340W	Affected. For details, please refer to the following URL. > <a href="https://www.ricoh.com/products/security/vulnerabilities/adv?id=ricoh-prod000168-2025-000007">https://www.ricoh.com/products/security/vulnerabilities/adv?id=ricoh-prod000168-2025-000007</a>
SP 230SFNw	Affected. For details, please refer to the following URL. > <a href="https://www.ricoh.com/products/security/vulnerabilities/adv?id=ricoh-prod000169-2025-000007">https://www.ricoh.com/products/security/vulnerabilities/adv?id=ricoh-prod000169-2025-000007</a>
M 340FW	Affected. For details, please refer to the following URL. > <a href="https://www.ricoh.com/products/security/vulnerabilities/adv?id=ricoh-prod000170-2025-000007">https://www.ricoh.com/products/security/vulnerabilities/adv?id=ricoh-prod000170-2025-000007</a>

This website uses cookies and other tracking technologies to enhance user experience and to analyze performance and traffic on our website. We also share information about your use of our site with our social media, advertising and analytics partners. If we have detected an opt-out preference signal then it will be honored. Further information is available in our [Cookie Policy](#).

Rejecting cookies may impact your experience on the website, such as playing YouTube videos. [Cookie Policy](#)

**The distribution URL of this page:**

<https://www.ricoh.com/products/security/vulnerabilities/vul?id=ricoh-2025-000007>

Please note that any copy or paraphrase of the text of this document that differs in content from the distribution URL link, or omits the URL, is an uncontrolled copy and may lack important information or contain factual errors.

[Home](#) > [Sustainability](#) > [Governance](#) > [Information Security](#) > [Product security](#) > [Information List by Vulnerability](#) > Vulnerability Information

About RICOH	Investor Relations	Sustainability	Technology	News
Vision	IR News	Environment	Development	News Release
Company Overview	Corporate Strategy Meeting	Society	Ricoh's Technology	Information Stories
Integrated Report	Business Briefing/ESG Briefing	Governance	RICOH Design	
Advertising /		Information Security		

This website uses cookies and other tracking technologies to enhance user experience and to analyze performance and traffic on our website. We also share information about your use of our site with our social media, advertising and analytics partners. If we have detected an opt-out preference signal then it will be honored. Further information is available in our [Cookie Policy](#).

Rejecting cookies may impact your experience on the website, such as playing YouTube videos. [Cookie Policy](#)

Returns

About RICOH



Investor Relations



Sustainability



Products



Technology



Support & Downloads



News



  
Page Top

This website uses cookies and other tracking technologies to enhance user experience and to analyze performance and traffic on our website. We also share information about your use of our site with our social media, advertising and analytics partners. If we have detected an opt-out preference signal then it will be honored. Further information is available in our [Cookie Policy](#).

Rejecting cookies may impact your experience on the website, such as playing YouTube videos. [Cookie Policy](#)

