



Sygnia Print Server 2 Vulnerabilities in Windows Instructions

[Home](#) » [Sygnia](#) » Sygnia Print Server 2 Vulnerabilities in Windows Instructions 

Sygnia



**GX Print Server 2 for the Versant 3100i/180i Press
GP Controller D01 for ApeosPro C810 Series
Revoria Flow PC11 for Revoria Press PC1120
Revoria Flow E11 for Revoria Press E1136/E1125/E1100
Security Update Guide
September, 30, 2024**

Contents

- 1 Vulnerability
- 2 Update Programs
- 3 Download Procedure
- 4 Install Procedure
- 5 Documents / Resources
- 5.1 References

Vulnerability

Microsoft Corporation has announced vulnerabilities in Windows®. There are measures to fix these vulnerabilities which must also be implemented for our products – GX Print Server 2 for the Versant 3100i/180i Press, ApeosPro C810 Series GP Controller D01, Revoria Flow PC11 for Revoria Press PC1120, Revoria Flow E11 for Revoria Press E1136/E1125/E1100. Please follow the below procedure to fix the vulnerabilities.

The following procedure is intended that a System Administrator of the GX Print Server can fix the vulnerabilities. The steps described below must be performed on the GX Print Server.

Update Programs

An Internet connection is required before proceeding. Access the following URL and download the updates.

Information Number of security essentials update		Information Number of security non-essentials update	
2024 Security Updates	2024/9	2024 Security Update	–

- Information Number of security essentials update: September,2024 Updates (Folder name)
Ignore the updates if you have already implemented “KB5005112”.
2021-08 Servicing Stack Update for Windows 10 Version 1809 for x64-based Systems (KB5005112)
- URL
<https://www.catalog.update.microsoft.com/Search.aspx?q=2aa60267-ea74-4beb-9da4-bcb3da165726>
- File Name
windows10.0-kb5005112-x64_81d09dc6978520e1a6d44b3b15567667f83eba2c.msu

Updates (Folder name)

2024- Windows 10 Version 1809 .09 x64 (KB5043050)

- URL
<https://www.catalog.update.microsoft.com/Search.aspx?q=d4fa5e2a-46e2-4152-8111-fe631ab72a53>
- File Name
windows10.0-kb5043050-x64_235e10ebbb4d07409bb14b704e46ad420d36b153.msu

Updates (Folder name)

2024-08 Cumulative Update for .NET Framework 3.5 and 4.7.2 for Windows 10 Version 1809 for x64 (KB5041913)

- URL
<https://www.catalog.update.microsoft.com/Search.aspx?q=3c140ead-a1b4-43eb-b076-542bfd87c54b>

- File Name

windows10.0-kb5041913-x64_b00cd2de1915f11b56c21d7001962f67854afe07.msu

Updates (Folder name)

Update for Microsoft Defender Antivirus antimalware platform – KB4052623 (Version 4.18.24080.9) – Current Channel (Broad)

- URL

<https://www.catalog.update.microsoft.com/Search.aspx?q=Update%20Microsoft%20Defender%20Antivirus%20antimalware%20platform%20current%20channel>

- File Name

[updateplatform.amd64fre_be692955ff204de7443faf0d036574c0f2a4b3f5.exe](#)

Security intelligence updates for Microsoft Defender Antivirus and other Microsoft antimalware

- URL

<https://www.microsoft.com/en-us/wdsi/defenderupdates>

- File Name

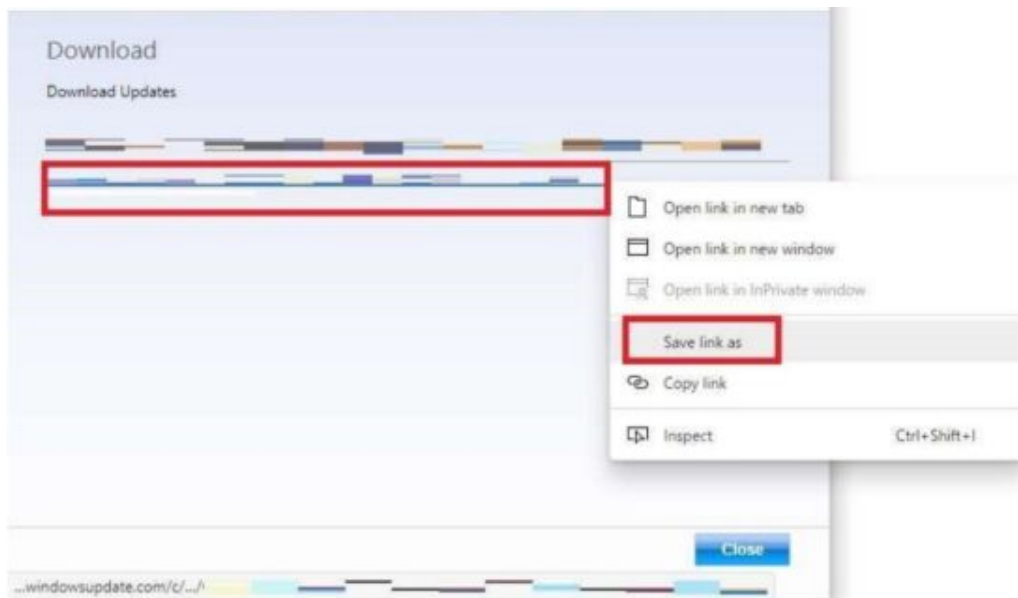
mpam-fe.exe

Download Procedure

1. Access above URLs with Microsoft Edge.
2. Click Download.



3. Right-click on the file name, select Save link as from the menu.



If there are more than one updates, perform the above step.

4. In the Save As screen, select the download destination for the updates, then click Save.
5. Updates will be saved to the location specified in Step (4).

Install Procedure

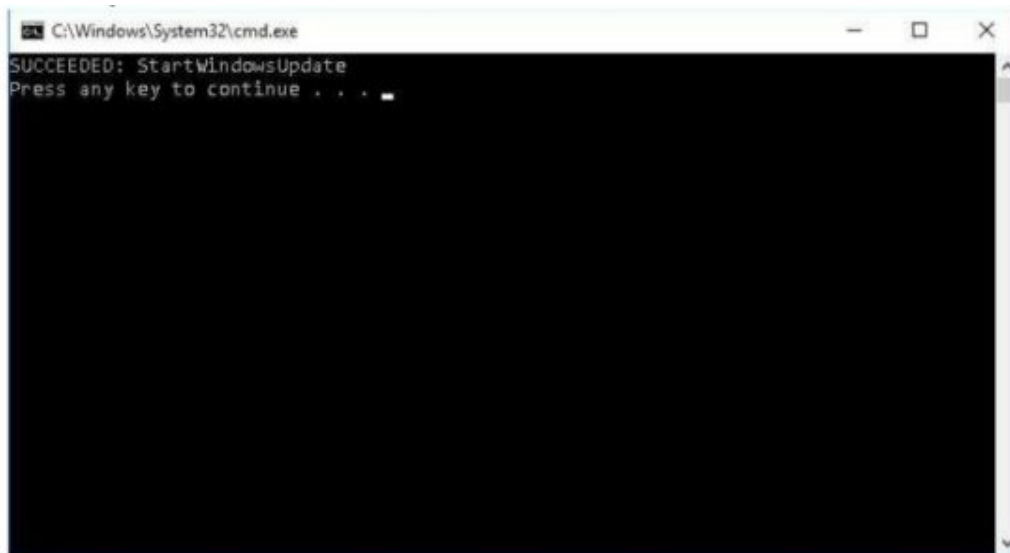
1. Preparation before Applying the Security Updates

1. Copy the update files to any folder on the GX Print Server.
2. Turn the power to the Print Server off and disconnect the network cable.



NOTE

- Metal parts are exposed on the back of the Print Server's main body.
 - When disconnecting the network cable be careful to avoid being injured by these parts.
 - Alternatively, you can disconnect the network cable on the hub side.
3. Turn the Print Server back on.
 4. If the Print Service application is running, then terminate it. (Windows Start menu > Fuji Xerox > StopSystem or Windows Start menu > FUJIFILM Business Innovation > StopSystem) Terminate any other running applications.
 5. Double-click on "D:\opt\PrtSrv\utility\ADMINtool\StartWindowsUpdate.bat".
 6. Press return key to continue.



2. How to Apply the Security Updates.

1. Double-click on the security update file.

Before applying the security update close all the running applications (e.g., Print Service).

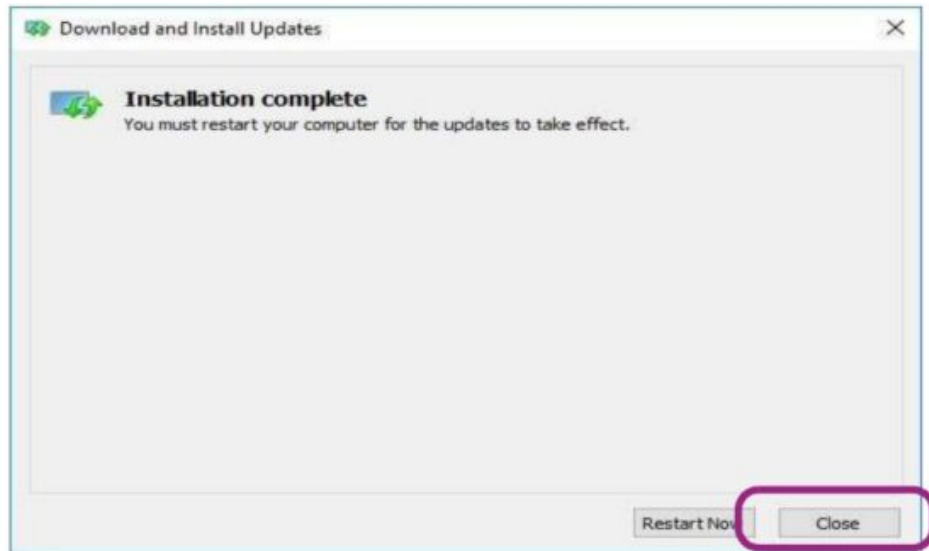
2. In the Windows Update Standalone Installer, click Yes.



3. The Installation will now begin.



- When the installation is finished, click Close to complete the setup.



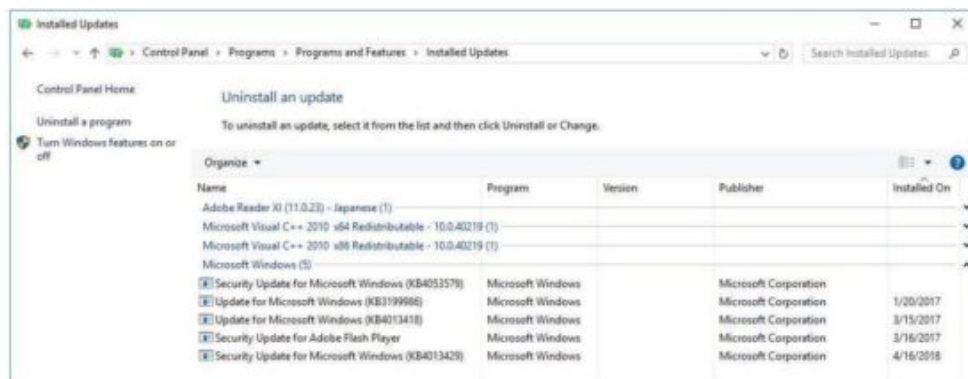
NOTE

You can reboot the computer every time a security update is applied.

3. Confirming the Security Updates.

By following the procedure described below you can confirm if the update programs have been successfully applied.

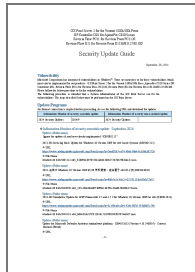
- Select Start Menu > Settings > Control Panel > Programs and Features.
- In the left pane click View installed updates.
- Confirm that the security updates that you applied are displayed in the list.



4. Completion

- Shut down the Print Server and reconnect the network cable.
- Turn the Print Server back on.

Sygnia

	Sygnia Print Server 2 Vulnerabilities in Windows [pdf] Instructions Versant 3100i, 180i Press GP Controller D01, ApeosPro C810 Series Revoria Flow PC11, Revo ria Press PC1120, Revoria Flow E11, Revoria Press E1136, E1125, E1100, Print Server 2 Vuln erabilities in Windows, Print Server 2, Vulnerabilities in Windows, Windows
--	---

References

-  [Microsoft Update Catalog](#)
-  [Microsoft Update Catalog](#)
-  [Microsoft Update Catalog](#)
-  [Microsoft Update Catalog](#)
-  [Microsoft Update Catalog](#)
-  [Latest security intelligence updates for Microsoft Defender Antivirus and other Microsoft antimalware - Microsoft Security Intelligence](#)
- [User Manual](#)

Manuals+, Privacy Policy

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.