Xerox Security Bulletin XRX18-011

Xerox® FreeFlow® Print Server v2.x on Windows®

Printers Supported: Xerox® Color C60/C70 Printer

Delivery of: Meltdown and Spectre Intel Design Flaw Patches
Bulletin Date: April 2, 2018

1.0 Background

This bulletin announces security patch deliverables for a Windows®-based FreeFlow® Print Server product to mitigate Meltdown and Spectre vulnerabilities announced by the US-CERT advisory council. These vulnerabilities are two different Central Processing Unit (CPU) flaws that affect hardware, software and the Windows Operating System. For more information on the Meltdown and Spectre vulnerabilities, refer to the Xerox URL below:

https://security.business.xerox.com/en-us/news/potential-vulnerability-affects-intel-processors/

These are vulnerabilities referred to as "speculative execution side-channel attacks" effecting modern processors (Intel, AMD and ARM) and operating systems such as Microsoft® Windows®. There are two components that must be applied to the FreeFlow® Print Server / Windows® platform to ensure that the Meltdown and Spectre vulnerabilities are mitigated. An install document is available to install these components. They are as follows:

1. **Windows Security Patches** (CVE-2017-5753 and CVE-2017-5754 per January 2018 Security Patch Update)
2. **Dell BIOS Firmware Update** (CVE-2017-5715 per Dell BIOS firmware update)

The January 2018 (or later) Security Patch Update must be installed on the FreeFlow Print Server platform to mitigate the vulnerabilities announced by CVE-2017-5753 and CVE-2017-5754. There are also Windows® registry settings that must be updated to complete the mitigation of these security vulnerabilities. The Dell BIOS firmware updates are installed from USB media to mitigate the vulnerability announced by CVE-2017-5715.

Microsoft and Dell claim that the Meltdown and Spectre mitigation updates (E.g., Windows® patches and BIOS firmware) may have performance impacts on the FreeFlow Print Server / Windows® platform. The FreeFlow® Print Server engineering team has run performance tests with these updates and found that there should be minimal to no impacts depending on the complexity of jobs being processed and printed.

The US-CERT advisory council announced three CVE's for the Meltdown and Spectre vulnerabilities.

Meltdown/Spectre Common Vulnerability Exposure (CVE) Table

US-CERT CVE	Type	CVE Description
CVE-2017-5753 Spectre Variant 1	bounds check bypass	Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
CVE-2017-5715 Spectre Variant 2	branch target injection	Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
CVE-2017-5754 Meltdown Variant 3	rogue data cache load	Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache.

Note: Microsoft® has discovered compatibility issues with some Anti-Virus (AV) software products. It is important to make sure that your AV software installed on the FreeFlow® Print Sever is the latest release and compatible with the Windows® kernel. See the information at the Microsoft® URL below:

https://support.microsoft.com/en-in/help/4072699/january-3-2018-windows-security-updates-and-antivirus-software

2.0 Applicability

The Meltdown and Spectre patches are available for all currently supported FreeFlow® Print Server platforms that are Windows®-based, and the Xerox printer products they support. This bulletin announces the mitigation of these vulnerabilities for the Xerox® Color C60/C70 Printer.

There are unique BIOS firmware updates for the different Dell platforms used as a Digital Front End (DFE) for the Xerox printer products. Other FreeFlow Print Server / Xerox printer products may support a different Dell platform configuration and therefore require their own unique BIOS firmware update.

2.1 Available Patch Update Install Methods

FreeFlow® Print Server security patch updates are available using a media (DVD/USB) and/or Internet Service (Update Manager or Windows Update) methods for the install. The FreeFlow® Print Server customer can schedule a Xerox Analyst or Service Engineer (CSE) to install a security patch update at a customer account. Xerox® offers the patch delivery available over the network from a Xerox server on the Internet using an application called Update Manager. Update Manager is a GUI-based application used to find available updates by selecting a '**Check for Updates**' option, and installing any listed updates found. The Analyst/CSE can choose to work with a customer, and allow them to install security patch updates from DVD/USB media, using the Update Manager UI (FreeFlow Print Server application), or using Windows® Update.

The customer has the option to install patches over the Internet from Microsoft using Windows® Update. This method has the advantage of retrieving Security patches at the soonest time possible. The Windows® Update method has most risk given the install of these Security patches directly from Microsoft® has not been tested on the FreeFlow® Print Server platform by Xerox®. Microsoft® does not deliver the Dell® BIOS firmware update required for Meltdown and Spectre mitigation, so this update is not available using the Windows® Update service. A Xerox CSE or Analyst must deliver the Dell® BIOS firmware update.

You cannot install the Dell® BIOS firmware update as part of the Meltdown and Spectre mitigation using the Update Manager UI or Windows® Update service. We are only making the Windows® patches available from the Update Manager UI by installing the January 2018 Security Patch Update (or later), or installing directly from Microsoft® using Windows® Update. The Spectre Variant #2 BIOS firmware update for the FreeFlow Print Server (Dell X86) platform must be installed from DVD/USB media. It is always good practice to first perform System Backup of the FreeFlow Print Server v2 / Windows® software, and archiving it to mitigate any risks of adverse impacts that could occur by installing security patch updates.

The use of Update Manager (GUI-based application) makes it simple for a customer to install Security patch updates. Downloading and installing Security Patch Updates using the Update Manager has the advantage of "ease of use" as it involves accessing the patch updates from a Xerox Server over the Internet. In addition, the FreeFlow® Print Server team performs testing of patch updates prior to releasing them to make sure that they do not cause any adverse impacts to job processing/printing, or render the printer inoperable.

2.2 Security Considerations

Security of the network devices and information on a customer network may be a consideration when deciding whether to use the DVD/USB, FreeFlow® Print Server Update Manager or Windows® Update method of patch delivery and install. When using Update Manager, the external Xerox server holding patch updates does not have access to the FreeFlow® Print Server platform at a customer location. The FreeFlow® Print Server platform (using Update Manager) initiates all communication over the Internet to download the Security patch, and the communication is "secure" using HTTP over the TSL 1.0 protocol (HTTPS on port 443) using an RSA 2018-bit certificate, SHA2 hash, and AES 256-bit stream encryption algorithms.

Delivery and install of the patch updates using the Update Manager UI may still be a concern for some highly "secure" customer locations such as US Federal and State Government sites. Alternatively, delivery and install of patch updates from DVD/USB media may be more desirable for high security sensitive customers. They can perform a security scan of the DVD/USB media with a virus protection application prior to install. If the customer

does not allow use of DVD/USB media for devices on their network, you can transfer (using SMB, SFTP, or SCP) patch updates to the FreeFlow® Print Server platform, and then install.

3.0 Patch Install

Xerox® strives to deliver critical Security patches in a timely manner. The customer process to obtain FreeFlow® Print Server patch updates is to contact the Xerox hotline support number. The methods of patch update delivery and install are over the Internet using Update Manager, directly from Microsoft® using Windows® Update service, and using DVD/USB media. It is always good practice to first perform System Backup of the FreeFlow Print Server v2 / Windows® software, and archiving it to mitigate risks of adverse impacts that could occur by installing these security patch updates.

We recommend the customer use the FreeFlow® Print Server Update Manager or Microsoft® Windows® Update method if they wish to perform install on their own. This empowers the customer to have the option of installing patch updates as soon as they become available, and not need to rely on the Xerox Service team. However, for the Meltdown and Spectre mitigation updates it is required to deliver and install the Dell BIOS firmware update (required for Spectre Variant #2) from DVD/USB media. Many customers do not want the responsibility of installing patch updates or they are not comfortable providing a network tunnel to the Xerox® or Microsoft® servers that store Security patches. In this case, the media install method is the best option under those circumstances.

3.1 DVD/USB Media Delivery

Xerox® uploads the FreeFlow® Print Server Security patch updates to a "secure" SFTP site that is available to the Xerox Analyst and Customer Service Engineer (CSE) once the deliverables have been tested and approved. The FreeFlow® Print Server patch deliverables are available as a ZIP archive or ISO image file, and a script used to perform the install for the media delivery method. Patch updates are installed by executing a script, and install on top of a pre-installed FreeFlow® Print Server software release. You can install Security patches from USB/DVD media, or from the FreeFlow® Print Server internal hard disk. A PDF document is available with procedures to install patch updates using the USB/DVD media delivery method.

The method used to install a patch update is copy or transfer the ZIP file update to a some directory location such as the Windows® Administrator home directory (C:\Users\Administrator), extract it, and then execute a script by typing the script name preceded by a dot and forward slash (E.g., ./<shell_script_name>).

If the Analyst supports their customer performing the patch updates, then they must provide the customer with the install document for the patch update and the security update deliverables. This method of patch update install is not as convenient or simple for customer install as the network install methods offered by Update Manger or Windows® Update.

3.2 Update Manager Delivery

The Update Manager is a GUI tool on the FreeFlow® Print Server platform used to check for security patch updates, download them, and install them. The customer can install FreeFlow® Print Server patch updates using the Update Manager UI, or schedule Xerox Service to perform the install. The Dell® BIOS firmware update required for mitigation of the Meltdown and Spectre vulnerabilities are not made available by the Update Manager UI.

Once Security patches are ready for customer delivery, we upload them to the Xerox communication server (a.k.a., Download Manager). Procedures are available for the System Administrator or Xerox Service to use the Update Manager UI to download and install Security patches over the Internet. The Update Manager UI has a '**Check for Updates**' button that can be selected to retrieve and list patch updates available from the Xerox communication server. When this option is selected the latest Security Patch Update should be listed (E.g., **January 2018 Security Patch Update for FreeFlow® Print Server v2**) as available for download and install. The Update Manager UI includes mouse selectable button options to download and then install the patches.

The customer proxy information is required to be setup on the FreeFlow® Print Server platform to access the patch updates over the Internet. The FreeFlow® Print Server platform initiates a "secure" communication session with the Xerox patch server using HTTP over the TSL 1.0 protocol (HTTPS on port 443) using an RSA 2018-bit certificate, and SHA2 hash, and AES 256-bit stream encryption algorithms. This connection ensures authentication of the FreeFlow® Print Server platform with the Xerox® communication server, and sets up encrypted communication for the patch data transfer. The Xerox® communication server does not initiate or have access to the FreeFlow® Print Server platform behind the customer firewall. The Xerox® communication server and FreeFlow® Print Server system both authenticate each other before making a connection between the two end-points, and performing the patch data transfer.

3.3 Microsoft Windows® Update Method

Another method to install the Security patches is directly from Microsoft using the Windows® Update service. Installing the Security patches directly from Microsoft using this service bring some risk given they have not been tested by Xerox on a FreeFlow® Print Server platform. It is required that the customer proxy server information be configured on the FreeFlow® Print Server platform so that it can gain access to the Microsoft server over the Internet outside of the customer network. The Dell BIOS firmware update required for mitigation of the Meltdown and Spectre vulnerabilities are not available using Windows® Update. You must retrieve the Dell BIOS firmware update, and prepare it on USB media for install.

We recommend manually performing a FreeFlow® Print Server System Backup and a Windows® checkpoint backup just prior to installing patches using the Windows® Update service. This will give assurance of FreeFlow® Print Server system recovery if installed Windows® OS patches create a software problem or results in the FreeFlow® Print Server / printer configuration becoming inoperable. Patch updates make changes to only the Windows® OS system/files, and not the FreeFlow® Print Server software. Therefore, the restore of a Windows® checkpoint will reverse install of the Security patches if recovery is required, and is much faster than the full System Restore from a System Backup. We recommend performing a full System Backup for redundancy purposes in case the checkpoint restore does not work.

4.0 Disclaimer

The information provided in this Xerox® Product Response is provided "as is" without warranty of any kind. Xerox® Corporation disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Xerox® Corporation be liable for any damages whatsoever resulting from user's use or disregard of the information provided in this Xerox® Product Response including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Xerox® Corporation has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential damages so the foregoing limitation may not apply.