Xerox Security Bulletin XRX18-020

Xerox® FreeFlow® Print Server v9 / Solaris® 11

Supported Printer Products:

- Xerox® Color 800i/1000i Digital Press
- Xerox® Versant® 3100 Press

Delivery of: Meltdown and Spectre Intel Design Flaw Patches
Bulletin Date: June 4, 2018

1.0 Background

This bulletin announces security patch deliverables for Solaris®-11 based FreeFlow® Print Server products 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 Solaris 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 Oracle® Solaris®. There are two components that must be applied to the FreeFlow® Print Server / Solaris® 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. **Solaris 11 Security Patches**
   - Addresses CVE-2017-5753 and CVE-2017-5754
   - April 2018 Security Patch Cluster includes patches.
   - Includes Firefox v52.7.3 Software
   - NVIDIA Graphic Driver
2. **Dell BIOS Firmware Update**
   - Addresses CVE-2017-5715
   - Must be installed from DVD or USB media.

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.

Oracle® and Dell® claim that the Meltdown and Spectre mitigation updates (E.g., Oracle® patches and BIOS firmware) may have performance impacts on the FreeFlow Print Server / Solaris® 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.

2.0 Applicability

The Meltdown and Spectre vulnerabilities apply to the FreeFlow® Print Server platforms and the Xerox® printer products below:

Release	Printer Product	DFE Controller
FFPS v9 / Solaris® 11	Versant® 3100 Press	Dell® T440 14G
	Xerox® Color 800i/1000i Press	Dell® T430 13G

There are unique BIOS firmware updates for the different Dell platforms used as a Digital Front End (DFE) for 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 Method

FreeFlow® Print Server security patch updates are available using a media (DVD/USB) method for 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. The Analyst/CSE can choose to work with a customer, and allow them to install security patch updates from DVD/USB media.

The Update Manager UI method of install over the network does not support download and install of Meltdown and Spectre patches. The April 2018 Security Patch Cluster is too large for support by Update Manager. You cannot install the Dell® BIOS firmware update as part of the Meltdown and Spectre mitigation using the Update Manager UI. It must be installed using the system BIOS session manager from DVD or USB media.

The Xerox Customer Service Engineer (CSE)/Analyst uses a tool that enables identification of the currently installed Solaris® OS version, FreeFlow® Print Server software version, Security Patch Cluster version, Java Software version and identification if the Solaris 11.3 Base Repository has been installed. This tool can be initially run to determine of the prerequisite Solaris® 11.3 OS and October 2017 Security Patch Cluster are currently installed, and also provides a status of the Meltdown and Spectre patch updates. Example output from this script for the FreeFlow® Print Server v9 software is as follows:

Solaris® OS Version:	11.3
FFPS Release Version	9.0_SP-3_(93.I0.04A.86)
FFPS Patch Cluster	April 2018
Java Version	Java 7 Update 181
Base Repository	Not Installed
Firefox Version:	52.7.3
Meltdown Variant #3	Installed
Spectre Variant #1	Installed
Spectre Variant #2	Installed

The above versions are the correct information after installing the April 2018 Security Patch Cluster and BIOS firmware update.

2.2 Security Considerations

Delivery and install of patch updates from DVD/USB media is a desirable method 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 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 method of patch update delivery and install for the Meltdown and Spectre patches is using DVD/USB media. It is always good practice to first perform System Backup of the FreeFlow Print Server v9 / Solaris® OS software, and archiving it to mitigate risks of adverse impacts that could occur by installing these security patch updates.

The Meltdown and Spectre patches are not supported for install using the Update Manager UI from the FreeFlow® Print Server platform. They can only be installed using DVD/USB media. The April 2018 Security Patch Cluster supports install from USB or the hard disk on the FreeFlow® Print Server. 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.

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 that has plenty of free space, extract it, and then execute a script by typing the script name preceded by a dot and forward slash (E.g., ./<shell_script_name>). These procedures are included in an install document available with the April 2018 Security Patch Cluster.

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 UI. It is always good practice to first perform System Backup of the FreeFlow Print Server v9.3 / Oracle® 11 OS software, and archiving it to mitigate any risks of adverse impacts that could occur by installing security patch updates.

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.

©2018 Xerox Corporation. All rights reserved. Xerox® and Xerox and Design®, FreeFlow®, Versant® are trademarks of Xerox Corporation in the United States and/or other countries.
BR21127

Other company trademarks are also acknowledged