

Xerox Security Bulletin XRX18-043

Xerox® FreeFlow® Print Server v7 / Solaris® 10
Supporting: Nuvera Printer Products



Delivery of: Meltdown and Spectre Intel Design Flaw Patches
Bulletin Date: November 29, 2018

1.0 Background

This bulletin announces security patch deliverables for Solaris®-10 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 patch updates for two components of the FreeFlow® Print Server / Solaris® 10 platform to ensure mitigation of the Meltdown and Spectre vulnerabilities. An install document is available to install patches for these components. They are as follows:

1. **Solaris® 10 OS Security patches**
 - a. Mitigation for:
 - CVE-2017-5753 (Spectre Variant #1)
 - CVE-2017-5754 (Meltdown Variant #3)
 - b. Available in the October 2018 Security Patch Cluster (or newer).
2. **BIOS Firmware update**
 - a. Mitigation for:
 - CVE-2017-5715 (Spectre Variant #2)
 - a. Available via SFTP site identified in the install document.
 - b. Install from bootable 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 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:

| Printer Product | Controller | BIOS Firmware File |
|--|----------------|--------------------|
| Nuvera® 100/120 Digital Copier/Printer | ITOX SB630-CRM | SB630B8A.31A |
| Nuvera® 100/120/144 Digital Production System | | |
| Nuvera® 100/120/144/157 EA Digital Production System | | |
| Nuvera® 200/288/314 EA Perfecting Production System | | |
| Nuvera® 100/120/144/MX Digital Production System | | |
| Nuvera® 200/288 MX Perfecting Production System | | |

Note: There are unique BIOS firmware updates for the different DFE Controller platforms used as a Digital Front End (DFE) for Xerox printer products.

2.1 Available Patch Update Install Method

The FreeFlow® Print Server security patch updates are available using a USB/DVD media method or using the Update Manger UI to download and install over the network. A 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.

The October 2018 Security Patch Cluster and later includes OS patches for Spectre Variant #1 and Meltdown Variant #3. The October 2018 Security Patch Cluster is made available on a Xerox communication server over the Internet by configuring the customer proxy server information on the FreeFlow® Print Server platform. The Update Manager UI can access the October 2018 Security Patch Cluster through from the Xerox communication server through the customer firewall. You cannot install the Dell® BIOS firmware update as part of the Meltdown and Spectre mitigation using the Update Manager UI. The BIOS firmware update must be installed from USB media using a bootable USB drive.

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 status of Meltdown and Spectre patches. This tool can be initially run to determine if the prerequisite October 2018 Security Patch Cluster or later is currently installed, and also provides a status of the Meltdown and Spectre patch updates. Example output from this script for the FreeFlow® Print Server v7 software is as follows:

```

Solaris OS Version:          10 Update 11
FFPS Release Version:      7.0_SP-3 (73.I1.51B.86)
FFPS Patch Cluster:        July 2018
Java Version:              Java 7 Update 181
Spectre Variant #1:        Not Installed
Meltdown Variant #3:      Not Installed
Spectre Variant #2:        Not Installed
  
```

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

2.2 Security Considerations

Delivery and install of a Security Patch Cluster 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 the Security Patch Cluster (using SFTP, or SCP) to the FreeFlow® Print Server platform, and then install from the hard disk. The BIOS firmware update must be installed from a bootable DOS formatted USB drive or DVD media depending on the Xerox printer product and supported Digital Front End (DFE) platform.

For network install, the customer proxy information is required to be setup on the FreeFlow® Print Server platform so it can access to the Security Patch Update over the Internet. The FreeFlow® Print Server platform initiates a “secure” communication session with the Xerox communication server using HTTP over the TLS 1.0 protocol (HTTPS on port 443) using an RSA 2048-bit certificate, SHA2 hash and AES 256-bit stream encryption algorithms. This connection ensures authentication of the FreeFlow® Print Server platform for the Xerox server, and sets up encrypted communication of the patch data. The Xerox server does not initiate or have access to the FreeFlow® Print Server platform behind the customer firewall. The Xerox server and FreeFlow® Print Server platform both authenticate each other before making a connection between the two end-points, and patch data transfer.

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 install methods available to install security patches is either from USB/DVD media or over the network using the Update Manger UI available from the FreeFlow® Print Server platform. However, install of the BIOS firmware for the Nuvera printer supported by FreeFlow® Print Server v7 / Solaris 10 is with a bootable USB drive.

It is always good practice to first perform System Backup of the FreeFlow® Print Server v7 / Solaris® OS software, and archiving it to mitigate risks of adverse impacts that could occur by installing a Security Patch Cluster. The System Backup can be used to restore the FreeFlow® Print Server and Solaris® 10 OS software if the patch install creates a software problem.

There are two patches available with the October 2018 Security Patch Cluster, which can be installed using either the DVD/USB or Update Manger methods. The Security Patch Cluster includes the Solaris® 10 OS patches for the Spectre Variant #1 and Meltdown Variant #3 vulnerabilities. The BIOS firmware update mitigates Spectre Variant #2, and is not available for installing using the Update Manager method over the network. This patch update must be installed from 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. These 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 USB/DVD media or the hard disk. The Security Patch Cluster is also made available from a Xerox communication server accessible for network install using the Update Manager UI on the FFPS platform. A PDF document is available with procedures to install a Security Patch Cluster using the USB/DVD media or Update Manager UI delivery methods. See **Section 2.2 “Security Considerations”** for information to determine if the install method chosen meets the security requirements and policies of a customer.

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. It is always good practice to first perform System Backup of the FreeFlow® Print Server v7.3 / Oracle® 10 OS software, and archiving it for purposes of recovery if a software issue occurs 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.

