Xerox Security Bulletin XRX18-009

Xerox® FreeFlow® Print Server (Solaris-based)

Supported Printer Products:

- All Xerox® Printers supported by Solaris®-based FreeFlow® Print Server

Delivery of: Meltdown and Spectre Intel Design Flaw Notification
Bulletin Date: March 6, 2018

1.0 Background

This bulletin announces the current Solaris®-based FreeFlow® Print Server product status with relation to the Meltdown and Spectre vulnerabilities for supported Xerox printer products. 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®. These are two different Central Processing Unit (CPU) flaws that impact hardware, software and the 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/

The solution for these vulnerabilities will be Oracle® Solaris® patches (Meltdown Variant 3 and Spectre Variant 1) and hardware BIOS firmware update (Spectre Variant 2). Oracle® and Dell® are still working on these updates, so the purpose of this document is to identify recommendations and tips to reduce Security risks of exploitation.

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.

< Continued on Next Page >

2.0 Applicability

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

Release	Printer Product	Latest DFE Controller	Predecessor DFE Controller
FFPS v9 / Solaris® 11	Versant® 3100 Press	Dell® T430 13G	None
	Xerox® Color 800i/1000i Press	Dellv T430 13G	None
FFPS v9 / Solaris® 10	iGen®4	Dell® T420i 12G	Dell® T610 11G
	iGen® 4 Diamond Edition®	Dell® T420i 12G	Dell® T610 11G
	iGen®150 Press	Dell® T420i 12G	Dell® T610 11G
	iGen® 8250 Press	Dell® T420i 12G	Dell® T610 11G
	Versant® 80/180 Press	Dell® Optiplex XE2 MT	None
	Versant® 2100 Press	Dell® T320 12G	None
	Color 800/100 Press	Dell® T420 12G	Dell® T610 11G
	Color 800i/1000i Press	Dell® T430 13G	Dell® T420 12G
	Color Press J75/C75 Press	Dell® Optiplex XE	None
	Color Press 560/570 Production Printer	Dell® Optiplex XE	None
	Impika® Compact Inkjet Press	X4-2 Motherboard	X3-2 Motherboard
	CiPress® 325/500 Production Inkjet System	X3-2 Motherboard	PIJ X4170 M2 Motherboard
	D95/110/125/136 Copier/Printer	Dell® Optiplex XE2 MT	Dell® Optiplex XE
FFPS v8 / Solaris® 10	iGen®4 Press	Dell® T420i 12G	Dell® T610 11G
	Color 800/1000 Press	Dell® T420 12G	Dell® T610 11G
	Color 560/570 Printer	Dell® Optiplex XE	Dell® T610 11G
	700/700i Digital Color Press	Dell® Optiplex XE	XS2440 Sun Ultra
	770 Digital Color Press	Dell® Optiplex XE	XS2440 Sun Ultra
FFPS v7 / Solaris® 10	Nuvera® 100/120 Digital Copier/Printer	SD630-H110 Motherboard	JD35Q Motherboard
	Nuvera® 100/120/144 Digital Production System	SD630-H110 Motherboard	JD35Q Motherboard
	Nuvera® 100/120/144/158 EA Digital Production System	SD630-H110 Motherboard	JD35Q Motherboard
	Nuvera® 200/288/314 EA Perfecting Production System	SD630-H110 Motherboard	JD35Q Motherboard
	Nuvera® 100/120/144 MX Digital Production System	SD630-H110 Motherboard	JD35Q Motherboard
	Nuvera® 200/288 MX Perfecting Production System	SD630-H110 Motherboard	JD35Q Motherboard
	DocuPrint® 100/115/135/155/180 MX EPS	Dell® Optiplex XE	Sun® Ultra 24
	DocuTech® 6115/6135/6180 Production Publisher	Dell® Optiplex XE	Sun® Ultra 24
	DocuTech® 128/155/180 Highlight Color Production Publisher	Dell® Optiplex XE	Sun® Ultra 24
	DocuColor® 240/250 Digital Color Printer/Copiers	PDSi 2B	W2100z
	DocuColor® 242/252/260 Digital Color Printer/Copiers	Sun® Ultra 24	PDSi 2B
	DocuColor® 5000AP/7000AP/8000AP Digital Press	ES5200	ES5100
	DocuColor® 7000/7002/8000/8002/8080 Presses	ES5200	ES5100
	Digital Printer 4112/4127 Enterprise Printing System	Dell® Optiplex XE	Sun® Ultra 24
	Digital 4590/4595 Copier/Printer	Dell® Optiplex XE	Sun® Ultra 24

There are unique BIOS firmware updates for the different Dell® platforms used as a Digital Front End (DFE) for the Xerox printer products in the above table.

2.1 Risk Management Recommendations and Suggestions

There is currently no known successful Meltdown or Spectre vulnerability exploitation of any Solaris® OS platforms to date. This information disclosure risk is possible for exploitation from Web services by remote browsers connecting over HTTP, and taking control from JavaScript. This risk can be eliminated for any FreeFlow® Print Server customer that does not require Web services for their print production workflow. Web services are commonly used for print workflows such as Internet Printing Protocol (IPP) job/status requests, Internet Web Client job/status requests, Scan to File and Scan Back features. In addition, Web services are also used for Remote Services (E.g., CFA data push, AMR, and Update Manager patch download). The Web services can be completely removed from the FreeFlow® Print Server platform to mitigate the risk of Meltdown and Spectre vulnerabilities if the above mentions workflows are not required by a customer.

We deliver quarterly Security Patch Clusters that remediate all known Common Vulnerability Exposures (CVE's) that are announced by the US-CERT advisory council. It is extremely important that customer ensure the latest Security Patch Cluster is installed on the FreeFlow® Print Server / Solaris® platform once they become available. The delivery of a Security Patch Cluster is announced at www.xerox.com from the "Security at Xerox" web page, and you can configure an RSS feed to receive Security bulletins that announce these deliverables.

There are many Security tightening controls that can be applied to the FreeFlow® Print Server platform. Contact your Xerox Analyst representative if you need assistance with Security controls. It is recommended to do the following:

1. Define the Security Profile in the FreeFlow® Print Server GUI as "High" to ensure services not needed for job workflows are disabled.

2. Disable all UDP/TCP ports not used for job workflows to minimize remote access to the printer. There is a Port Management tool bundled with the FFPS software. Also apply the IP Filter option by defining a list of IP addresses for remote devices that will require access to the Xerox printer.

3. We recommend removal of the Firefox Mozilla browser packages from the FreeFlow® Print Server / Solaris platform. Firefox Mozilla includes vulnerabilities that can allow exploitation of the Meltdown and Spectre vulnerabilities.

4. If a customer requires any of the Remote Service capabilities (such as CFA data push, AMR, or eCare) for the Nuvera printer the removal of Firefox Mozilla impacts setup of customer proxy information. However, the proxy information can be configured using alternative methods.

5. Install the high-volume Xerox printer products in a secure physical location only accessible by a limited number of trusted people. The FreeFlow® Print Server software platform is installed by a Xerox Customer Service Engineer (CSE/) or Analyst. They must be a trusted person given this is the point at which malicious software can be installed.

6. We recommend that the customer limit System Administrator (SA) access to the FFPS GUI to trusted personal, and keep SA access very limited to as few people as possible. Also limit root account access to the underlying platform to the most trusted person. Enable the Strong Password feature and define Password Security parameters to your site user account Security policies.

7. We recommend that the customer does not install any applications on the FreeFlow® Print Server platform. This is a specialized Digital Front End (DFE) controller with very tightly controlled applications for the purpose of managing, processing and printing jobs. There is limited risk with these very specialized and controlled set of services. Applying solid Security principles are recommended to reduce risk of Meltdown or Spectre exploitation.

8. It is also highly recommended to enabled audit logging services on the FreeFlow® Print Server / Solaris® platform. Key audit logging services that can be configured and enabled are Basic Security Model (BSM), Solaris® System Logging (syslog) and FreeFlow® Print Server GUI Console logging. For BSM and syslog can be enabled by assigning the Security profile to "High", and the Console GUI logging is enabled from the FreeFlow® Print Server GUI. It is the responsibility of the customer to review the audit logs at a periodic time frame to analyze for suspicious activity.

2.2 Meltdown and Spectre Patch Delivery

Once the Meltdown and Spectre solutions (Solaris® OS patches and Dell® BIOS firmware update) are available they will be delivered using a DVD/USB media and Update Manager network delivery method. FreeFlow® Print Server Security patch updates are available for a delivery method using media (DVD/USB) for the install. The FreeFlow® Print Server customer schedules a Xerox Analyst or Service Engineer (CSE) to install the Security patches at the customer account. The Analyst/CSE can choose to work with a customer, and allow them to install the Security patches from DVD/USB media.

Xerox® offers Security patch updates over the network from a Xerox server using an application called FreeFlow® Print Server Update Manager. 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 Security Patch Update from a Xerox Server over the network. If you decide to remove Web services from the FreeFlow® Print Server platform to mitigate the Meltdown and Spectre vulnerabilities the Update Manager application will be inoperable. In this case the DVD/USB media delivery method can be used to install the Meltdown and Spectre patches and BIOS firmware update.

2.3 Patch Delivery 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 or Update Manager method of Security patch delivery and install. When using Update Manager, the external Xerox server that includes the Security patch updates does not have access to the FreeFlow® Print Server platform at a customer site. The FreeFlow® Print Server platform (using Update Manager) initiates all communication to download the Security patch update, and the communication is "secure" by SSL over port 443 with the Xerox server. 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 2018-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.

Delivery and install of the Security patches using Update Manager may still be a concern for some highly "secure" customer locations such as US Federal and State Government sites. Alternatively, delivery and install of Security patches from DVD/USB media may be more desirable for these highly 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) the Security Patch Update to the FreeFlow® Print Server platform, and then install.

3.0 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.