Xerox Security Bulletin XRX17-015

Xerox® FreeFlow® Print Server (Solaris-based Products)

Common Vulnerability Exposure: CVE-2017-7494

Vulnerability Area: Samba Remote Code Execution Vulnerability

Bulletin Date: June 22, 2017

A. Background

Oracle® responds to US CERT advisory council notifications of Security vulnerabilities referred to as Common Vulnerabilities and Exposures (CVE's) and develops patches that remediate the Security vulnerabilities are applicable to Solaris® 10 OS and components (e.g., Apache, Samba, OpenSSH, etc.). This bulletin is announcing a critical high-risk remote code execution vulnerability in the Samba component on certain FreeFlow® Print Server platforms installed with Samba version 3.5.0 or higher. This remote code execution vulnerability enables a malicious client to upload a shared library to a writable share on the FreeFlow® Print Server platform, so that the server loads and executes it.

The FreeFlow® Print Server organization has a dedicated development team, which actively reviews the US CERT advisory council CVE notifications, and delivers Security patch updates from Oracle® to remediate the threat of these Security risks for the FreeFlow® v7, v8 and v9 platforms. The FreeFlow® Print Server engineering team retrieves the vendor Security patch that mitigates the high-risk vulnerability, and tests prior to delivery for customer install.

We deliver a Security Patch Cluster on a quarterly sequence (January, April, July, and October). A prerequisite to install of the Samba patch that mitigates the remote code execution vulnerability is install of the latest April 2017 Security Patch Cluster. Once the April 2017 Security Patch Cluster you can install the Samba patch for CVE-2017-7494. We will include this patch in the next quarterly scheduled July 2017 Security Patch Cluster.

Note: Xerox recommends that customers evaluate their security needs periodically and if they need Security patches to mitigate Common Vulnerability Exposures, schedule an activity with their Xerox Service team to install the latest Security Patch Cluster. The customer can manage their own Security Patches using the methods described in Section C "Patch Install", but we recommend checking with Xerox Service to reduce risk of installing patches that have not tested by Xerox.

B. Applicability

This bulletin is applicable to all Xerox printer products managed by the FreeFlow® Printer Server application running on the Solaris 10 Operating System. It only applies to the FreeFlow® Print Server platforms that incorporate the Samba 3.5.0 software or higher. The FreeFlow® Print Server software has a utility to identify the current version of installed applications (SMB, FireFox, Patch Cluster, Java, etc.). Use this utility to determine if the installed Samba packages are v3.5.0 or newer, and if so this CVE-2017-7494 SMB patch is applicable for install.

A prerequisite for installing the CVE-2017-7494 SMB patch is the April 2017 Security Patch Cluster installed on the FFPS platform. Use the utility that identifies the current Security Patch Cluster version to determine the current version installed on the FreeFlow® Print Server platform. Install the April 2017 Security Patch Cluster if not currently installed. If the Security Patch Cluster is newer than April 2017 there is no need to install the CVE-2017-7494 SMB patch. It is already included in the newer Security Patch Cluster.

The CVE-2017-7494 SMB patch is applicable for a wide range of Xerox printer products managed by the FreeFlow® Print Server platform. Make sure that the FreeFlow® Print Server version installed is the latest for each major release (E.g., 7.3, 8.2 and 9.3) to ensure existence of the latest Solaris 10 OS. See the applicable Xerox printer products and the FreeFlow® Print Server major release supported below:

FreeFlow® Print Server v7.3

FreeFlow® Print Server v7.3 software release managing the Xerox printer products below:

1. Xerox Nuvera® 100/120/144/157 EA Digital Production System
2. Xerox Nuvera® 200/288/314 EA Perfecting Production System
3. Xerox Nuvera® 100/120/144 MX Digital Production System
4. Xerox Nuvera® 200/288 MX Perfecting Production System
5. Xerox® DocuPrint 100/115/135/155/180 MX Enterprise Printing System
6. Xerox® DocuTech® 6128/6155/6180 Production Publisher
7. Xerox® DocuTech® Highlight Color 128/155/180 Production Publisher
8. Xerox® DocuColor® 242/252/260/700,
9. Xerox® DocuColor® 5000AP
10. Xerox® DocuColor® 7002/8002
11. Xerox® DocuColor® 8080
12. Xerox® Digital Printer 4112/4127 Enterprise Printing System
13. Xerox® Digital 4590/4595 Copier/Printer

FreeFlow® Print Server v8.2

FreeFlow® Print Server v8.2 software release managing the Xerox printer products below:

1. Xerox iGen®4 Press
2. Xerox® Color 560/570 Printer
3. Xerox ® 700i/700 Digital Color Press

FreeFlow® Print Server v9.3

FreeFlow® Print Server v9.3 software release managing the Xerox printer products below:

1. Xerox® iGen® Products (iGen4, iGen150, Xerox® Color 8250 Presses)
2. Xerox® Versant 80/2100 Presses
3. Xerox® Color 800/100, 800i/1000i Presses
4. Xerox® Color Press J75/C75 Presses
5. Xerox® Color Press 560/570
6. Xerox® Impika® Compact Inkjet Press
7. Xerox® CiPress® 325/500 Production Inkjet System
8. Xerox® Rialto® 900 Inkjet Press
9. Xerox® D95/110/125/136 D95/110/125/136 Copier/Printers

C. Patch Install

Xerox strives to deliver Security Patches in a timely manner. The customer process to obtain FreeFlow® Print Server Security Patch deliverables is to contact the Xerox hotline support number. Xerox® provides a method of Security Patch delivery and install are over the network using the FreeFlow® Print Server Update Manager. Alternatively, Xerox delivers the Security Patches for install from DVD/USB media.

We recommend customer use the FreeFlow® Print Server Update Manager method if installing patches on their own. This empowers customers with the option to install these patch updates at time of availability, and not need to rely on the Xerox Service team. Many customers do not want the responsibility of installing Security patches and prefer Xerox Service to install. There are customers not comfortable providing a network tunnel to the Xerox servers that store the Security Patches. In this case, the media install method is the best option under those circumstances. See a more detailed description of the Security Patch Update delivery methods with the information below:

i. FreeFlow Print Server Update Manager Delivery

FreeFlow® Print Server Update Manager is a GUI tool on the FreeFlow® Print Server platform used to check for, download and install Security updates. The customer can install quarterly Security Patches using the FreeFlow® Print Server Update Manager UI, or schedule Xerox Service to perform the install.

Once the Security patches are ready for customer delivery, they are available from the Xerox Edge Host and Download servers. Procedures are available for the FreeFlow® Print Server System Administrator or Xerox Service for using the Update Manager GUI to download and install the 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 patch server. When this option is selected the Security Patch name should be listed (E.g., "**CVE-2017-7494**: Samba Remote Code Execution Patch") as available for download and install. The Update Manager UI includes mouse selectable buttons to download and then install patches.

Xerox uploads the FreeFlow® Print Server Security Patch deliverables to a Xerox patch server that is available on the Internet outside of the Xerox Corporate network once the deliverable has been tested and approved. Once in place on the Xerox server, a CSE/Analyst or the customer can use FreeFlow® Print Server Update Manager UI to download and install on the FreeFlow® Print Server platform.

The customer proxy information is required to be setup on the FreeFlow® Print Server platform so it can access to the Security Patch deliverable over the Internet. The FreeFlow® Print Server platform initiates a "secure" communication session with the Xerox patch server using HTTP over the TSL 1.2 protocol (HTTPS on port 443) using an RSA 2018-bit certificate, and SHA1 encryption. 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 system both authenticate each other before making a connection between the two end-points, and patch data transfer.

ii. DVD/USB Media Delivery

Xerox uploads the FreeFlow® Print Server Security Patch deliverables to the Customer Field Operations (CFO) Web site that is available to the Xerox Analyst and Service 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. The Security Patches install by executing a script, and installs on top of a pre-installed FreeFlow® Print Server software release. The install script include options to install the Security Patch deliverable directly from DVD/USB media or from the FreeFlow® Print Server internal hard disk. A PDF document is available with procedures to install the Security Patch Update using the DVD/USB media delivery method upon request.

If the Analyst supports their customer performing the Security Patch install, then they must provide the customer with the Security Patch install document and the Security Patch deliverables. This method of Security Patch install is not as convenient or simple for customer install as the network install method offered by the FreeFlow® Print Server Update Manger.

D. 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 FreeFlow® Print Server Update Manager delivery and install method of Security Patches. The external Xerox server that includes the Security Patches 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 FreeFlow® Print Server Security Patch deliverable, and the communication is "secure" by SSL over port 443 with the Xerox server.

Delivery and install of the Security Patch Update using FreeFlow® Print Server 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 Patch Updates 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.

E. 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.