Xerox Security Bulletin XRX18-002

Xerox® FreeFlow® Print Server v2.1 on Windows

Supported Printers:

Xerox® iGen®5 Press

Delivery of: Security Profile Settings Updates and Vulnerability Mitigations
Bulletin Date: January 17, 2018

1.0 Background

This bulletin announces a FreeFlow® Print Server v2 platform set of Security Profile setting updates and Security vulnerability mitigations. The Security Profile has a "High" configuration option, which configures settings on the FreeFlow® Print Server platform to provide protection of customer Personally Identifiable Information (PII) and Personal Health Information (PHI), and other type of malicious attacks. The Security profile setting updates announced by this bulletin are intended to apply stronger Security techniques and settings. The default Security profile is "Standard", and when changing the option to "High" the new Security settings are applied. The applied settings are as follows:

1. The FreeFlow® Print Server platform has been updated with the TLS 1.2 cryptographic module and a patched OpenSSH 7.3 cryptographic module. With these module updates you can configure an SSL Certificate that uses SHA2 and AES 256-bit encryption. The SHA2 hash and AES 256-bit stream algorithms are the strongest encryptions options today.

   Once you define the Security profile to "High", TLS 1.2, SHA2 hash encryption, and AES 256-bit encryption options are configured on the FreeFlow® Print Server platform.

   A suite of strong Ciphers and MACs are supported by the TLS 1.2 and Secure Shell (SSH) modules. The suite of Ciphers and MACs supported are as follows:

Ciphers Supported	MACs Supported
3des-cbc,blowfish-cbc	ecdh-sha2-nistp256
cast128-cbc,arcfour	ecdh-sha2-nistp384
arcfour128	ecdh-sha2-nistp521
arcfour256	diffie-hellman-group-exchange-sha256
aes128-cbc	diffie-hellman-group-exchange-sha1
aes192-cbc	diffie-hellman-group14-sha1
aes256-cbc	diffie-hellman-group1-sha1
rijndael-cbc@lysator.liu.se	
aes128-ctr	
aes192-ctr	
aes256-ctr	
aes128-gcm@openssh.com	
aes256-gcm@openssh.com	
chacha20-poly1305@openssh.com	

2. Digital Signing is a Security feature in the SMB protocol that digitally signs packets communicated between an SMB client/server. By default, the FreeFlow® Print Server / Windows® software install enables SMB v1/v2 services and disables digital signing of SMB packets. SMB Digital Signing is enabled on the FreeFlow® Print Server platform when the Security profile is set to "High", SNMP v1/2 are disabled, and SNMP v3 is enabled. Digital Signing of SMB packets prevents man-in-the-middle attacks.

3. By default, SNMP v1/v2 is enabled on the FreeFlow® Print Server platform. Defining the Security profile to "High" disabled SMMB v1/v2 and enable SNMP v3, which are secure job and printer status services. SNMP v3 adds much stronger security features than SNMP v1/v2, such as client authentication, encryption of credentials, and encryption of bidirectional SNMP traffic. SNMP v3 ensures "secure" remote monitoring of Xerox printers for IPv4 and IPv6 network addressing. FreeFlow® Print Server supports two implementations of SNMP (Net-SNMP and Epilog Envoy) and both of these support Trap Services. The ports used by the SNMP services are port 161 (Net-SNMP v3 Services) port162 (Trap Services), and port 16611 (Epilogue v1/v2 Services).

4. By default, the Windows Remote Desktop is enabled and remotely accessible on the FreeFlow® Print Server platform. Defining the Security profile to "High" will disable Windows Remote Desktop so that it cannot be remotely accessed. You can define a custom Security profile from the built-in "High" profile to enable Windows Remote Desktop that is secure with an SSL certificate, and strong encryption algorithms.

This bulletin also announces Open Source updates and software changes to mitigate Security vulnerabilities announced by the US-CERT advisory council and/or reported by Security scanner applications. The FreeFlow® Print Server platform updates to mitigate Security vulnerabilities are as follows:

1. The Apache HTTP services have been updated to the latest 2.4.27 version to address serious vulnerabilities such as the TLS/SSL Birthday attacks on 64-bit block ciphers per CVE-2016-2183. Legacy block ciphers having block size of 64 bits are vulnerable to a practical collision attack when used in CBC mode. All versions of SSL/TLS protocol support cipher suites which use DES or 3DES as the symmetric encryption cipher are affected.

2. The example Apache Tomcat Servlet / JSP Container default files are removed from the FreeFlow® Print Server platform. These files can be used by a malicious attacker to uncover information about the installed Tomcat services, and these files can contain cross-site scripting vulnerabilities. The removal of these files mitigates these risks.

3. The chargen service is disabled on the FreeFlow® Print Service to prevent a potential malicious attacker from spoofing packets between computing devices running this service. A simple attack referred to as ping-pong is possible, which causes two computing devices to transmit characters at each other impacting their performance, and the performance of the network. This service is no longer used so does not impact print workflow when disabled.

4. The HTTP trace/track methods are disabled on the FreeFlow® Print Service to prevent a malicious attacker from creating a TRACE request that captures the client's cookies and result in a cross-site scripting attack.

5. We have modified the Apache HTTP configuration to restrict proxy requests to only host 10.40.101.30 for internal networks. This is mitigation for the "HTTP Proxy Arbitrary Site/Port Relaying" vulnerability, which is a weakness that can lead to rogue interactive sessions opened through the HTTP proxy.

< Continued on Next Page >

2.0 Applicability

The Security Profile Settings Updates and Vulnerability Mitigation patches are available for the FreeFlow® Print Server v2 software and standalone configuration for the Xerox components below:

1. Xerox® iGen®5 Press
2. FreeFlow® Print Server 23.0.17214.0

2.1 Available Patch Update Install Methods

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 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 the Security patch delivery available 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 patches using the Update Manager has the advantage of "ease of use" as it involves accessing the Security patches from a Xerox Server over the network.

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 method of Security patch delivery and install. When using Update Manager, the external Xerox server that includes the Security patch update 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 patches, and the communication is "secure" by SSL over port 443 with the Xerox server.

Delivery and install of 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. The customer 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.

< Continued on Next Page >

3.0 Patch Install

Xerox® strives to deliver these critical Security Patch updates in a timely manner. The customer process to obtain FreeFlow® Print Server Security patches is to contact the Xerox hotline support number. The methods of Security Patch delivery and install are over the network using FreeFlow® Print Server Update Manager, and using media (i.e., DVD/UB).

We recommend the customer use the FreeFlow® Print Server Update Manager 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. Many customers do not want the responsibility of installing Security patches or they are not comfortable providing a network tunnel to the Xerox® server that store the 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 patches to a "secure" SFTP 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 installs by executing a script, and installs on top of a pre-installed FreeFlow® Print Server software release. The Security patches can be installed 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.

The most common method to install a shell script patch is copy or transfer it to a directory created under the C:\Users\Administrator directory (Windows Administrator home directory), and then execute the 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 Security patch install, then they must provide the customer with the Security patch install document and the Security update deliverables. This method of Security patch install is not as convenient or simple for customer install as the network install methods offered by Update Manger.

3.2 Update Manager Delivery

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

Once Security patches are ready for customer delivery, they are available from the Xerox communication servers. Procedures are available for the FreeFlow® Print Server System Administrator or Xerox Service for using 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 patch server. When this option is selected a list of updates should be listed (E.g., **Valid for all regions - IGEN5_23.0.17214.0_SECURITY_PATCH_BUNDLE**) 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 so it can access to the Security patches 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 2048-bit certificate, and SHA2 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 performing the patch data transfer.

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.