Xerox Product Security

The Heartbleed OpenSSL Vulnerability

Version 1.9

July 1, 2014 - Updated

Disclaimer

The information provided in this document 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 document 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.

The information in this bulletin is subject to change without notice.

Table of Contents

Introduction

A vulnerability has been discovered in the OpenSSL cryptographic software version **1.0.1** to **1.0.1f** widely used across the Internet for banking, investment, medical and other encrypted network traffic. The Heartbleed OpenSSL vulnerability works by allowing the certificate checking to be corrupted and traffic across a network to be monitored and some have called eavesdropping. Obviously, this presents quite a large problem for anything done with encryption, especially over the Internet. This document lists the Xerox products and whether or not they are affected by this issue.

An Important Point

This document contains products that Xerox currently sells and some that they have recently stopped selling. If your product is not listed, it is probably older and therefore would have a version of OpenSSL that is not susceptible to this vulnerability. The first vulnerable version of OpenSSL was made available in April of 2012. Therefore a Xerox device acquired on or before April of 2012 is not vulnerable.

Legend for Product Tables

A third column with the explanations is provided below. The remainder of the document each table has only two columns.

Type of Product	Affected	Meaning
Product Name	NO	Product Not Affected by Vulnerability
Product Name	YES	Product Affected by Vulnerability
Product Name	UI	Product Under Investigation
Product Name	Details	Product requires more Details

Hardware Products

Monochrome Product Table

Monochrome Models	Affected
Phaser® 3010	NO
Phaser® 3040	NO
Phaser® 3250	NO
Phaser® 3320 **Updated Software on Support Web Site**	Fixed
Phaser® 3610	NO
Phaser® 3635	NO
Phaser® 4510	NO
Phaser® 4600/4620	NO
Phaser® 5550	NO
Phaser® 6125	NO
WorkCentre® 3210/3220	NO
WorkCentre® 3315	NO
WorkCentre® 3325 **Updated Software on Support Web Site**	Fixed
Phaser® 3635MFP	NO
WorkCentre® 3045	NO
WorkCentre® 3615	NO
WorkCentre® 4150	NO
WorkCentre® 4250/4260	NO
WorkCentre® 5135/5150	NO
WorkCentre® 5325/5330/5335	NO
WorkCentre® 5632/5638/5645/5655/5665/5675/5687	NO
WorkCentre® 5740/5745/5755/5765/5775/5790	NO
WorkCentre® 5845/5855/5865/5875/5890	NO
Xerox® D95/D110/D125® Copier/Printer	NO
Xerox® D136® Copier/Printer and Printer	NO
DocuPrint® 425/850, 500/1000, 525/1050CF	NO
Xerox 495 CF (Continuous Feed)	NO
Xerox 650/1300 CF (Continuous Feed)	NO

**Recommended Actions*

If your Xerox printer or multifunction has YES in the Affected column, here's what you should do to protect yourself against the Heartbleed vulnerability.

1. Determine if your device is directly connected to the Internet or is behind a firewall or router. A firewall or router is recommended to cut down on the possibility of attack from external sources.
2. Assess your risk profile. As mentioned above, direct connection to the Internet may have already exposed your device to attack. But if your device is only visible to your internal network and your network users are unlikely to know about or have taken advantage of this vulnerability you may choose to do nothing at this time.
3. Otherwise, if you suspect you have been or could be attacked, determine if SSL/HTTPS is currently enabled. If you are part of a managed services program with Xerox such as MPS or PagePack then SSL/HTTPS will be enabled. In other cases, it may or may not be. Note: If you are part of a managed services program, please contact your Xerox representative before changing this setting.
    a. Set port 443 (SSL/HTTPS) to disabled. This completely prevents the vulnerability from being exploited. Note: This will prevent Web Services (Automatic Meter Reads, or Network Scanning Validation Service) and remote administration from running.
    b. Change any passwords associated with this device or have been part of documents that were previously printed using the device.
4. Monitor http://www.xerox.com/heartbleedbug for information regarding an update for your device. Additional instructions will be provided on how to install this update and some additional steps you will need to take once the update is installed.

Color Product Table

Color Models	Affected
Phaser® 6010	NO
Phaser® 6015	NO
Phaser® 6128/6128MFP	NO
Phaser® 6130	NO
Phaser® 6140	NO
Phaser® 6180/6180MFP	NO
Phaser® 6280	NO
Phaser® 6360	NO
Phaser® 6400	NO
Phaser® 6500	NO
Phaser® 6600	NO
Phaser® 6700	NO
Phaser® 7100	NO
Phaser® 7400	NO
Phaser® 7500	NO
Phaser® 7800	NO
Phaser® 8560/8560MFP	NO
ColorQube® 8570/8870	NO
ColorQube® 8700/8900 Xerox ConnectKey Controller	NO
ColorQube® 8700/8900	NO
ColorQube® 9201/9202/9203	NO
ColorQube® 9201/9202/9203	NO
ColorQube® 9301/9302/9303 Xerox ConnectKey Controller	NO
WorkCentre® 6015	NO
WorkCentre® 6505	NO
WorkCentre® 6605	NO
ColorQube® 8700	NO
ColorQube® 8900	NO
WorkCentre® 3550	NO
WorkCentre® 6400	NO
WorkCentre® 7120/7225	NO
WorkCentre® 7220/7225	NO
WorkCentre® 7328/7335/7345/7346	NO
WorkCentre® 7425/7428/7435	NO
WorkCentre® 7525/7530/7535.7545/7556	NO
WorkCentre® 7655/7665/7675	NO
WorkCentre® 7755/7765/7775	NO
WorkCentre® 7830/7835/7845/7855	NO
Xerox Color 550/560/570®	NO
Xerox Color C75/J75 Press®	NO

Color Models	Affected
Xerox Wide Format 6279 **Patch to be Available 2014**	UI
Xerox Wide Format 6705 **Patch to be Available 2014**	UI
Xerox Wide Format IJP2000 **Patch to be Available 2014**	UI

Software Products MPS/XOS Tools

Managed Services Product Table

Managed Services Software	Affected
Xerox Device Agent	NO
Xerox Device Agent Partner Edition	NO
Xerox Device Agent (iPad and Print Portal)	NO
Xerox Device Agent (XDA and XDA_SeS)	NO
Xerox Integration Servers	NO
Xerox Report Manager	NO
PagePack Assistant	NO
PagePack Local Assistant	NO
Xerox Profit & Loss Tool	NO
Xerox Services Manager Data Warehouse	NO
Auto Update Server	NO
Non Xerox Pricing Tool	NO
Tandoori	NO
Xerox Incident Killer	NO
Xerox Custom Authentication Server	NO
Xerox Office Productivity Advisor Import Tool	NO
Xerox Web Packager	NO
Xerox License Manager	NO
Xerox Asset Manager	NO
Xerox Help Desk	NO
SmartSend	NO
Xerox Export Agent	NO
Xerox Mobile Print Portal	NO
Xerox Services Manager Contract Adapter	NO
Page Pack Assistant	NO
Page Pack Local Assistant	NO
Xerox Production Imaging Manager	NO
MPS Contractibility Catalog	NO
Xerox Print Awareness Tool	NO
AssetDB	NO
Smarter Configuration Optimizer	NO
Xerox Device Manager	NO
Xerox Job Ticket	NO
Xerox Models Database	NO
Xerox Mobile Print	NO
Xerox Optimization Tool	NO

Managed Services Software	Affected
Xerox Services Portal	NO
Fleet Management Portal / PagePack Center	NO
Managed Print Service API	NO
Print Services Sales Tool	NO
Xerox Device Data Collector	NO
Xerox Models & Pricing Server	NO
Xerox Print Agent	NO
Xerox Print Awareness	NO
Xerox Services Manager	NO
Xerox Transformation Manager	NO

Mobile Print Products Table

General Markets Software	Affected
Xerox Mobile Print Cloud (All Versions)	NO
Xerox Mobile Print Cloud Agent (All Versions)	NO
Xerox Mobile Print Enterprise (All Versions)	NO
Xerox Mobile Print Portal (All Versions)	NO
Xerox Mobile Print Solution (All Versions)	NO

General Markets Product Table

General Markets Software	Affected
Xerox Device Agent Lite	NO
CentreWare® Web	NO

Web Content Product Table

Web Content Software	Affected
Xerox DocuShare®	NO
Xerox Content Management Services	NO

Fire Records Management System

Application Name	Affected
FH7 Fire Records Management	NO
FHnet Fire Records Management	NO
FHMedic Records Management	NO

Software Products Operations Tools

Xerox Office Solutions

Application Name	Affected
NSi AutoStore v6	NO
NSi Output Manager	NO
Equitrac for MPS	NO
Equitrac Express	NO
Copitrak	NO
Xerox AutoStore v5	NO
Xerox Scan to PC Desktop - Nuance	NO
Scan to Cloud	NO
Cloud Connector	NO
Nuance eCopy ShareScan	NO
Nuance Scan Flow Store	NO
eCopy	NO
SafeCom	NO
PaperPort	NO
OmniPage	NO
Copitrak	NO
PrinterOn	NO
Xerox Secure Access V4	NO
Xerox Secure Access V5	NO
Xerox SMARTDocument Travel v5	NO

Extensive Interface Platform (EIP)

Application Name	Affected
EIP Platform 2.5	NO
EIP Platform 3.0	NO
EIP SDK	NO
EIP SDK 2.5	NO
EIP SDK 3.0	NO
Info App 1.0	NO
Scan to Email App 1.0	NO
Scan to FTP App 1.0	NO
Scan to MultiDest App 1.0	NO
Scan to SharedFolder App 1.0	NO
Scan to USB App 1.0	NO
Xerox App Development Suite	NO
Xerox App Studio	NO

FreeFlow Print Server Table

FFPS Software	Affected
FreeFlow® Print Server Versions 7.X, 8.X and 9.X	NO
FreeFlow® Print Server Versions that use Solaris/Oracle 10.X (Repaired by Oracle patch)	NO

FreeFlow Application Table

FreeFlow Applications Software	Affected
FreeFlow® Core	NO
Open Automation Platform of FreeFlow® Core	NO
FreeFlow® Digital Publisher	NO
FreeFlow® Express to Print	NO
FreeFlow® Fleet Navigator	NO
FreeFlow® Makeready™	NO
FreeFlow® Output Manager™	NO
FreeFlow® Process Manager™	NO
FreeFlow® Print Manager™ Advanced Print Path	NO
FreeFlow® Variable Information Suite	NO
FreeFlow VI Compose	NO
FreeFlow VI Design Express	NO
FreeFlow VI Design Pro	NO
FreeFlow VI eCompose	NO
FreeFlow VI eCompose Dispatch SDK	NO
FreeFlow VI Explorer	NO
FreeFlow VI Projects Manager	NO
FreeFlow VI VIPP Manage	NO
FreeFlow Web Services (Partner)	NO
FreeFlow VI Compose	NO
GMC IntegratedPLUS Solution	NO
Xerox® IntegratedPLUS Automated Color Management	NO
Xerox® IntegratedPLUS Finishing Solution	NO
ProfitQuick™	NO

Connectkey

Application Name	Affected
ConnectKey for DocuShare	NO
ConnectKey for SharePoint	NO
ConnectKey Share to Cloud	NO

Xerox.com Systems

Account Management Applications

As of Sunday, April 13th, Xerox servers have been patched and protected against the Heartbleed Bug. Our recommendation is to change your password, now that our environment has been remediated.

Note: Xerox.com identity management has a single sign-on, therefore you only need to change your password once for all listed account management applications.

Application Name	Previously Vulnerable	Patch loaded	Action Recommended
Meter Reads	YES	YES	Change password
Metered Supplies	YES	YES	Change password
Automatic Supplies Replenishment	YES	YES	Change password
My Supplies	YES	YES	Change password
MySupport	YES	YES	Change password
Online Invoicing – payment system	YES	YES	Change password
Recycling (GWA- Green World Alliance)	YES	YES	Change password
eBuyout	YES	YES	Change password
Order Status	YES	YES	Change password
Support & Drivers	YES	YES	Change password
Loyalty Program / Xerox Genuine Rewards	YES	YES	Change password
Purchase Order Management	YES	YES	Change password
Find Your Sales Rep	YES	YES	Change password
eCommerce (Open Market, private web ordering portals)	YES	YES	Change password

To change your password please visit:
United States- https://www.accounts.xerox.com/auth/remind.jsf?locale=en_US
Canada (English)- https://www.accounts.xerox.com/auth/remind.jsf?locale=en_CA
Canada (French)- https://www.accounts.xerox.com/auth/remind.jsf?locale=fr_CA

Other Web-based and Managed Print applications

Application Name	Previously Vulnerable	Patch loaded	Action Recommended
Xerox Direct / Xerox Shop	NO	N/A	None
Xerox Europe Partner Configurator, Price lists, and SAVE	NO	N/A	None
Xerox Europe Online Supplies Store	NO	N/A	None
Xerox Europe Genuine Rewards	NO	N/A	None
Simple Secure Sign-on (S3)	NO	N/A	None
Xerox Partner Print Services (XPPS)	NO	N/A	None
European Reseller Accreditation	NO	N/A	None
European Trade-in	NO	N/A	None
European Reseller Easy Cashback	NO	N/A	None
European End User Offer claim system	NO	N/A	None
Reseller sites	YES	YES	Change password
Service Partner Tools and Resources	YES	YES	Change password
Service Contract Ordering Tool (SCOT)	YES	YES	Change password
Authorized Service Delivery	YES	YES	Change password
Authorized Service Providers	YES	YES	Change password
Xerox Remote Print Services (XRPS)	YES	YES	Change password
eConcierge	YES	YES	Change password
Free Color Printers	YES	YES	Change password
eStore	NO	N/A	None
Xerox Business Innovation Partner Portal	NO	N/A	None
Xerox Developer Portal	NO	N/A	None
Xerox Survey System	NO	N/A	None
XPPGN Registration System	NO	N/A	None