Xerox Product Security

FREAK OpenSSL Vulnerability

Version 1.4

August 14, 2015
Original publish date May 27, 2015

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 in the OpenSSL library for SSL/TLS has been reported. It can allow an attacker to execute a man-in-the-middle attack against vulnerable systems that support older key exchange methods. This vulnerability is called FREAK for “Factoring attack on RSA-EXPORT Keys”. OpenSSL versions prior to 0.9.8zd, 1.0.0p, or 1.0.1k may allow attackers to conduct downgrade attacks and facilitate brute-force decryption on weak (512 bit) RSA keys.

Exploiting this vulnerability requires both a vulnerable client and server along with a server that reuses keys, a dedicated attacker and access to computing resources to break the key. Attacks are most likely to occur in places with public network access such as airports or shops that provide WiFi hotspots.

This problem affects very few cases as shown below.

- Microsoft Windows (all versions, client or servers) are not affected as that Operating System normally uses its own encryption solution and not OpenSSL.
- Apple Macintosh users of some mobile versions and desktop operating systems could be vulnerable.
- Linux clients or server versions are able to upgrade to a non-vulnerable OpenSSL easily using the APT or RPM Package Management tools.
- Solaris client or server versions are able to upgrade to a non-vulnerable OpenSSL easily using the dpkg Package Management tool

Beyond showing that many Operating Systems are not vulnerable or can be easily protected, it is very unlikely that an attacker could predict and be ready to act at the precise moment when two vulnerable devices are communicating. This document lists Xerox products and whether 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, please contact Xerox technical support for further information.

Legend for Product Tables

A third column with the explanations is provided below. For 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	**Fixed**	**Current linked SW is not affected.**
Product name	**Yes**	**Product affected by vulnerability**

Monochrome Models	Affected	Est. Patch Availability Date
DocuPrint® 425/850, 500/1000, 525/1050CF	Yes*	TBD
Phaser® 3010/3040	Yes*	TBD
Phaser® 3155/3160	Yes*	TBD
Phaser® 3250	No	N/A
Phaser® 3610	Yes*	TBD
Phaser® 3635 MFP Patch software available here.	Fixed	NOW
Phaser® 4600/4620	Yes*	TBD
Phaser® 5335	Yes*	TBD
WorkCentre 3550	Yes*	TBD
WorkCentre® 3045 B/NI	Yes*	TBD
WorkCentre® 3210/3220	No	N/A
WorkCentre® 3615	Yes*	TBD
WorkCentre® 3655 Patch Software available here.	Fixed	NOW
WorkCentre® 4150	No	N/A
WorkCentre® 4250 Patch software available here.	Fixed	NOW
WorkCentre® 4260 Patch software available here.	Fixed	NOW
WorkCentre® 5135/5150	Yes*	TBD
WorkCentre® 5632/5638/5645/5655/5665/5675/5687	Yes*	TBD
WorkCentre® 5735/5740/5745/5755/5765/5775/5790 Patch software available here.	Fixed	NOW
WorkCentre® 5845/5855/5865/5875/5890 ConnectKey Patch Software available here.	Fixed	NOW
WorkCentre® 5945/5955 Patch Software available here.	Fixed	NOW
WorkCentre® 6655 Patch Software available here.	Fixed	NOW

Color Models	Affected	Est. Patch Availability Date
ColorQube® 8700/8900 Xerox ConnectKey Controller Patch Software available here.	Fixed	NOW
ColorQube® 9201/9202/9203 CBC Patch software available here.	Fixed	NOW
ColorQube® 9201/9202/9203 SBC Patch software available here.	Fixed	NOW
ColorQube® 9301/9302/9303 Xerox ConnectKey Controller Patch Software available here.	Fixed	NOW
Phaser® 6000/6010	Yes*	TBD
Phaser® 6125	No	N/A
Phaser® 6128/6128MFP	No	N/A
Phaser® 6130	No	N/A
Phaser® 6140	No	N/A
Phaser® 6180/6180MFP	No	N/A
Phaser® 6280	No	N/A
Phaser® 6500	Yes*	TBD
Phaser® 6600	Yes*	TBD
Phaser® 6700 Patch Software available here.	Fixed	NOW
Phaser® 7100	Yes*	Never
Phaser® 7800 Patch Software available here.	Fixed	NOW
WorkCentre® 3550	Yes*	TBD
WorkCentre® 6015 N/NI	Yes*	TBD
WorkCentre® 6400	Yes*	11/20/2015
WorkCentre® 6505	Yes*	TBD
WorkCentre® 6605	Yes*	TBD
WorkCentre® 7220/7225 Xerox ConnectKey Controller Patch Software available here.	Fixed	NOW
WorkCentre® 7525/7530/7535/7545/7556	Fixed	NOW
WorkCentre® 7655/7665/7675	Yes*	TBD
WorkCentre® 7755/7765/7775	Fixed	NOW
WorkCentre® 7830/7835 ConnectKey Controller Patch Software available here.	Fixed	NOW
WorkCentre® 7845/7855 ConnectKey Controller Patch Software available here.	Fixed	NOW
WorkCentre® 7970 ConnectKey Controller Patch Software available here.	Fixed	NOW

*Recommended Actions

1. If your Xerox printer or multifunction has Yes* in the Affected column, the below steps indicate what you should do to protect yourself against the FREAK vulnerability.
2. Determine if your Xerox device is networked to a server or client that has a vulnerable version of OpenSSL. As noted earlier in this document, if the client you are using is a Microsoft Windows version, those operating systems do not use OpenSSL and, therefore, will not have this vulnerability.
3. For an Apple Macintosh mobile or desktop client, check for the version number and see if an upgrade is available and apply it.
4. For Linux clients, upgrading OpenSSL to 0.9.8zd or 1.0.1p or newer with the APT or RPM systems will eliminate this issue. For Solaris clients or servers, you may use dpkg or automated update to upgrade. If print servers are being used, the version of OpenSSL (if used) should be upgraded as possible. Client-to-client and server-to-server communications may be affected by this.
5. If possible, upgrade all clients and servers.
6. If it is not possible to upgrade all clients snd servers, you may wish to have them not communicate with a vulnerable Xerox device or disconnect them from the network.
7. Monitor http://www.xerox.com/security 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.