Xerox Product Security

The Man-In-The-Middle (MITM) OpenSSL Vulnerability

Version 1.1

September 19, 2014

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

Table of Contents i

Introduction 2

An Important Point 2

Legend for Product Tables 2

Hardware Products 3

Monochrome Product Table 3

*Recommended Actions 3

Color Product Table 4

Introduction

A vulnerability has been discovered in the OpenSSL cryptographic software versions **0.9.8 – 0.9.8z** and **1.0.1-1.0.1g** widely used across the Internet for banking, investment, medical, and other encrypted network traffic. It is fixed in **0.9.8za** and **1.0.1h**. The Man-In-The-Middle (MITM) OpenSSL vulnerability works by forcing the use of weak keys that allow an attacker via a Man-In-The-Middle attack to decrypt and modify traffic from a vulnerable client or server.

Note: **The attack may only be performed between a vulnerable client and a vulnerable server. There is a very good explanation by InfoWorld's Paul Venezia about how unlikely it is for this attack to occur:** **http://www.infoworld.com/d/data-center/the-new-openssl-flaw-no-heartbleed-243861**

A vulnerability was reported in OpenSSL versions 0.9.8 – 0.9.8z and 1.0.1-1.0.1g that allow a Man-In-The-Middle attack. The attack would require that both hosts have a vulnerable version of OpenSSL.

This problem affects very few cases as shown below.

- Microsoft Windows (all versions, client or servers) are not affected as that Operating System uses a different encryption tool.
- Apple Macintosh users (all versions, clients or servers) are not affected as that Operating System uses a different encryption tool.
- 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, it is probably older and, therefore, would have a version of OpenSSL that is not susceptible to this vulnerability. The first version of OpenSSL with this vulnerability was made available in 2005.

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	**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® 3010/3040	Yes*
Phaser® 3155/3160	Yes*
Phaser® 3250	Yes*
Phaser® 3320	Yes*
Phaser® 3610	Yes*
Phaser® 3635 MFP	Yes*
Phaser® 4510	Yes*
Phaser® 4600/4620	Yes*
Phaser® 5335	Yes*
Phaser® 5550	Yes*
Phaser® 6125	No
WorkCentre® 3210/3220	Yes*
WorkCentre® 3315/3325	Yes*
Phaser® 3635MFP	Yes*
WorkCentre® 3045 B/NI	Yes*
WorkCentre 3550	Yes*
WorkCentre® 3615	Yes*
WorkCentre® 4150	No
WorkCentre® 4250/4260	Yes*
WorkCentre® 5135/5150	UI
WorkCentre® 5325/5330/5335	UI
WorkCentre® 5632/5638/5645/5655/5665/5675/5687	UI
WorkCentre® 5740/5745/5755/5765/5775/5790 Updated Software on Support Web Site	Fixed
WorkCentre® 5845/5855/5865/5875/5890 Xerox ConnectKey Controller Updated Software on Support Web Site	Fixed
Xerox® D95/D110/D125® Copier/Printer	Yes*
Xerox® D136® Copier/Printer and Printer	Yes*
DocuPrint® 425/850, 500/1000, 525/1050CF	Yes*
Xerox 495CF	No
Xerox 650/1300CF	No

*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 Man-In-The-Middle (MITM) vulnerability.
2. Determine if your Xerox device is networked to a 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 or an Apple Macintosh, those operating systems do not use OpenSSL and, therefore, will not have this vulnerability. For Linux clients, upgrading OpenSSL to 0.9.8za or 1.0.1h 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.
3. If possible, upgrade all clients and servers.
4. If it is not possible to upgrade all clients, you may wish to have them not communicate with a vulnerable Xerox device or disconnect them from the network.
5. Monitor http://www.xerox.com/Man_in_The_Middle-bug 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® 6000/6010	Yes*
Phaser® 6015	Yes*
Phaser® 6125	No
Phaser® 6128/6128MFP	No
Phaser® 6130	No
Phaser® 6140	No
Phaser® 6180/6180MFP	No
Phaser® 6280	No
Phaser® 6360	Yes*
Phaser® 6400	Yes*
Phaser® 6500	Yes*
Phaser® 6600	Yes*
Phaser® 6700	Yes*
Phaser® 7100	Yes*
Phaser® 7400	Yes*
Phaser® 7500	Yes*
Phaser® 7800	Yes*
Phaser® 8560/8560MFP	Yes*
ColorQube® 8570/8870	Yes*
ColorQube® 8700/8900 Xerox ConnectKey Controller Updated Software on Support Web Site	Fixed
ColorQube® 9201/9202/9203	Yes*
ColorQube® 9301/9302/9303 Xerox ConnectKey Controller Updated Software on Support Web Site	Fixed
WorkCentre® 6015 N/NI	Yes*
WorkCentre® 6505	Yes*
WorkCentre® 6605	Yes*
WorkCentre® 3550	No
WorkCentre® 6400	Yes*
WorkCentre® 7120/7225	UI
WorkCentre® 7220/7225 Xerox ConnectKey Controller Updated Software on Support Web Site	Fixed
WorkCentre® 7328/7335/7345/7346	UI
WorkCentre® 7425/7428/7435	UI
WorkCentre® 7525/7530/7535.7545/7556	Yes*
WorkCentre® 7655/7665/7675	Yes*
WorkCentre® 7755/7765/7775	Yes*
WorkCentre® 7830/7835/7845/7855 Xerox ConnectKey Controller Updated Software on Support Web Site	Fixed
Xerox Color 550/560/570®	UI
Xerox Color C75/J75 Press®	Yes*