Mini Security Bulletin XRX14D

Release Date: Jun 10 2014 Version 1.0

Purpose

Inform our Xerox Customers of an issue that has minor security implications.

Last week 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 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 tools

Beyond showing that many Operating Systems are not vulnerable or can be easily protected, it is extremely unlikely that an attacker could predict and be ready to act at the precise moment when two vulnerable devices are communicating.

Xerox is in the process of investigating which of our products are affected and will provide more information and software upgrades as they become available.