Security Bulletin XRX19-015

Xerox® WorkCentre® 5325/5330/5335
Xerox® Color 550/560 Printer
Xerox® Color C60/C70
Xerox® D95/D95A/D110/D125 Copier/Printer
Xerox® D136 Copier/Printer
Xerox® Versant® 180/3100 Press
All Xerox® VeraLink® Devices

Address Cipher-Block-Chaining Mode Cipher Suite Vulnerabilities

Bulletin Date: July 12, 2019
Update: July 22, 2019

Background

Servers that utilize TLS1.0, TLS1.1, and TLS1.2 with Cipher-Block-Chaining mode cipher suites enabled are susceptible to man-in-the-middle attacks that exploit MAC padding.

To mitigate this vulnerability on Xerox print systems that do not support disabling CBC mode ciphers make sure that the device is setup in a secure environment. In addition:

1. Ensure the system is behind a network firewall.
2. Provide physical security controls to limit access to the network from an internal location.
3. Always install the most current software/firmware versions.

For Xerox print systems that do support disabling CBC ciphers, make sure that the servers communicating with these Xerox print systems are configured to disallow use of CBC mode.

No upgrade of any system software release is required to address these man-in-the-middle attacks for the products indicated below.

Applicability

The mitigation steps mentioned above apply to the network-connected versions for the following products:

Xerox WorkCentre	Xerox Color	Xerox	Xerox Versant
5325	550	D95	180
5330	560	D95A	3100
5335	C60	D110	
	C70	D125	
		D136	

In addition, these mitigations apply to all VersaLink devices.

The solution for these vulnerabilities is classified as Critical.