KONICA MINOLTA

Security Advice

Ripple20

Version: 1.0

Date: July 21, 2020

Knowledge Article: RFEU_BT2016916EN

BEU Service and Support Division

Giving Shape to Ideas

Table of Contents

1 Background

On June 16th, 2020 JSOF published their “Ripple20” vulnerability report. The report lists 19 vulnerabilities in the TCP/IP stack from “Treck Inc.”, which is specially developed for embedded systems.

https://www.jsof-tech.com/ripple20/

2 Potential risk scenarios

- An attacker from outside the network taking control over a device within the network, if internet facing.
- An attacker who has already managed to infiltrate a network can use the library vulnerabilities to target specific devices within it.
- An attacker could broadcast an attack capable of taking over all impacted devices in the network simultaneously.
- An attacker may utilize affected device as a way to remain hidden within the network for years
- A sophisticated attacker can potentially perform an attack on a device within the network, from outside the network boundaries, thus bypassing NAT configurations. This can be done by performing a MITM attack or a DNS cache poisoning.
- In some scenarios, an attacker may be able to perform attacks from outside the network by replying to packets that leave network boundaries, bypassing NAT

3 Possible mitigation

- minimize network exposure for affected devices by disabling not needed protocols
- ensure that devices are not accessible from the Internet, unless absolutely essential
- Secure the network environment in which the device is located with a firewall
- Use of the IP filter function to restrict access

4 Product Status

4.1 Office Printing

	Konica Minolta	affected	fix schedule
A3 – Color	bizhub C759/C659	no	
	bizhub C754e/C654e	no	
	bizhub C754/C654	no	
	bizhub C658/C558/C458/C368/C308/C258	no	
	bizhub C554e/C454e/C364e/C284e/C224e	no	
	bizhub C554/C454/C364/C284/C224	no	
	bizhub C650i/C550i/C450i/C360i/C300i/C250i	no	
	bizhub C287/C227	no	
A3 – B&W	bizhub 958/758	no	
	bizhub 754e/654e	no	
	bizhub 754/654	no	
	bizhub 558/458/368/308	no	
	bizhub 554e/454e/364e/284e/224e	no	
	bizhub 367/287/227	no	
	bizhub 306/266	no	
	bizhub 246i/226i/206i	no	
	bizhub 226	no	
	bizhub 225i	no	

	Konica Minolta	affected	fix schedule
A4 – Color	bizhub C3100P	no	
	bizhub C3110	no	
	bizhub C3851FS/C3851/C3351	no	
	bizhub C3850FS/C3850/C3350	no	
	bizhub C3350i/C4050i/C3300i/C4000i	no	
	bizhub C4020i/C3320i	no	
A4 – B/W	bizhub 4752/4052	no	
	bizhub 4750/4050	no	
	bizhub 4422/3622	no	
	bizhub 4020/3320	no	
	bizhub 4702P/4402P/3602P	no	
	bizhub 4700P/4000P/3301P	no	
	bizhub 5020i/4020i/5000i/4000i	yes	under investigation
	bizhub 3080MF/3000MF/2600P	yes	under investigation

4.2 Production Printing

	Konica Minolta	affected	fix schedule
PP – Color	AccurioPress C6100/C6085	no	
	AccurioPress C3080/C3080P/C3070 AccurioPrint C3070L	no	
	AccurioPress C2070/2070P/C2060 AccurioPrint C2060L	no	
	bizhub PRESS C7000/C7000P/C6000 bizhub PRO C7000/C6000/C6000L	no	
	bizhub PRESS C8000	no	
	bizhub PRESS C1100/C1085	no	
	bizhub PRESS C1070/1070P/C1060 bizhub PRO C1060L	no	
PP – B/W	AccurioPress 6136/6136P/6120	no	
	bizhub PRESS 1250/1250P/1052 bizhub PRO 951	no	
	bizhub PRO 1100	no	
	Bizhub PRESS 2250P	no	

4.3 Industrial Printing

	Product	affected	fix schedule
IP	KM-1	under investigation *1)	
	JETvarnish 3D	under investigation *2)	
	JETvarnish 3D Evolution	under investigation *2)	
	JETvarnish 3D One	under investigation *2)	
	JETvarnish 3D Web	under investigation *2)	
	JETvarnish 3DS	under investigation *2)	
	Meteor Unlimited Colors Se+ (DP8700 SE+ with iFOIL)	under investigation *2)	
	Accurio Label 230	no	
	Accurio Label 190	no	

*1) **KM-1**: Under investigation if PLC's (programmable logic controller) using TRECK TCP/IP stack. PLC's are connected to a separated internal network and have no connection to the outside network, therefore the risk of exploiting the vulnerabilities is very low.

*2) **Jet Varnish series / Meteor**: Under investigation if internal components use TRECK TCP/IP stack. For connection to customers network a dedicated port at the PC WorkStation is used, which is not affected by the vulnerability.

The system uses a separated internal network to connect all components. They will have no connection to the outside network, therefore the risk of exploiting the vulnerabilities is very low.