



KONICA MINOLTA

# Security Advice

## Service Location Protocol Vulnerability

CVE-2023-29552

Version: 1.2

Date: May 2<sup>nd</sup>, 2023

International Service

Information Classification

IC1 – None/Public

Konica Minolta Business Solutions Europe GmbH  
Information Security

Table of Contents

1 Change Log ..... 3

2 Background ..... 4

3 Konica Minolta Product Status ..... 5

4 Mitigation..... 6

# 1 Change Log

Version	Date	Modification
1.0	26/04/2023	Initial version
1.1	28/04/2023	Added mitigation workflow for IT6 and device manual links
1.2	02/05/2023	Added list of applications not using SLP & CVSS score

## 2 Background

Recently, researchers from Bitsight and Curesec have discovered a way to abuse the Service Location Protocol (SLP) - identified as CVE-2023-29552, to conduct high amplification factor DoS attacks using spoofed source addresses.

The SLP allows an unauthenticated remote attacker to register arbitrary services. Attackers exploiting this vulnerability could leverage vulnerable instances to launch massive Denial-of-Service (DoS) amplification attacks with a factor as high as 2200 times, potentially making it one of the largest amplification attacks ever reported.

SLP is a protocol that was created in 1997 through RFC 2165 to provide a dynamic configuration mechanism for applications in local area networks. SLP allows systems on a network to find each other and communicate with each other. It does this by using a directory of available services, which can include things like printers, file servers, and other network resources. SLP works by having a system register itself with a directory agent, which then makes that system's services available to other systems on the network. Daemons providing SLP are bound to the default port 427, both UDP and TCP. SLP was not intended to be made available to the public Internet.

CVE ID	Affected Function	Potential Impact	CVSSv3.1 Score	Countermeasure
CVE-2023-29552	Service Location Protocol	Denial of Service	8.6	Mitigation below

**Reference:** [Service Location Protocol Vulnerability \(Bitsight\)](#)

Since the SLP is included in most Konica Minolta devices, we would like to bring this security advice to your attention. Please refer to "Konica Minolta Product Status" for device impact and mitigation.

### 3 Konica Minolta Product Status

The vulnerability CVE-2023-29552 is affecting the Service Location Protocol (SLP) itself. Devices that either have this protocol disabled or have it enabled but are not directly accessible via the public Internet (i.e behind a firewall) are not directly at risk.

Devices that have the protocol enabled and are directly accessible via public Internet are at high risk and can be exploited by an attacker to carry out a Denial of Service (DoS) on a victims device/server.

The following is a list of applications that are not utilizing the Service Location Protocol:

- Box Operator
- CS Remote Care Data Collection Agent (CSRC DCA)
- CS Remote Care Relay Tool
- RSA Edge Installer
- Data Administrator
- FleetRMM
- Font Management Utility
- HDD BackUp Utility
- HDD TWAIN Driver
- IWS Deployment Tool
- Log Management Utility
- "PageScope Enterprise Suite
  - Net Care Device Manager
  - Account Manager
  - Authentication Manager
  - My Print Manager
  - My Panel Manager
  - Device Plug-ins"
- Print Status Notifier
- Real Time Mode TWAIN Driver
- Remote Deployment Tools (RDT)
- Tools for LK-114
  - ManagerPort
  - InstallerCreateTool
  - SetupTool"
- OpenAPI SDK
- bizhub Remote Panel (Remote Panel Server)
- CS Remote Care (Server modules)
- CS Remote Analysis (Server module)
- YSoft SafeQ 6
- Dispatcher Paragon

## 4 Mitigation

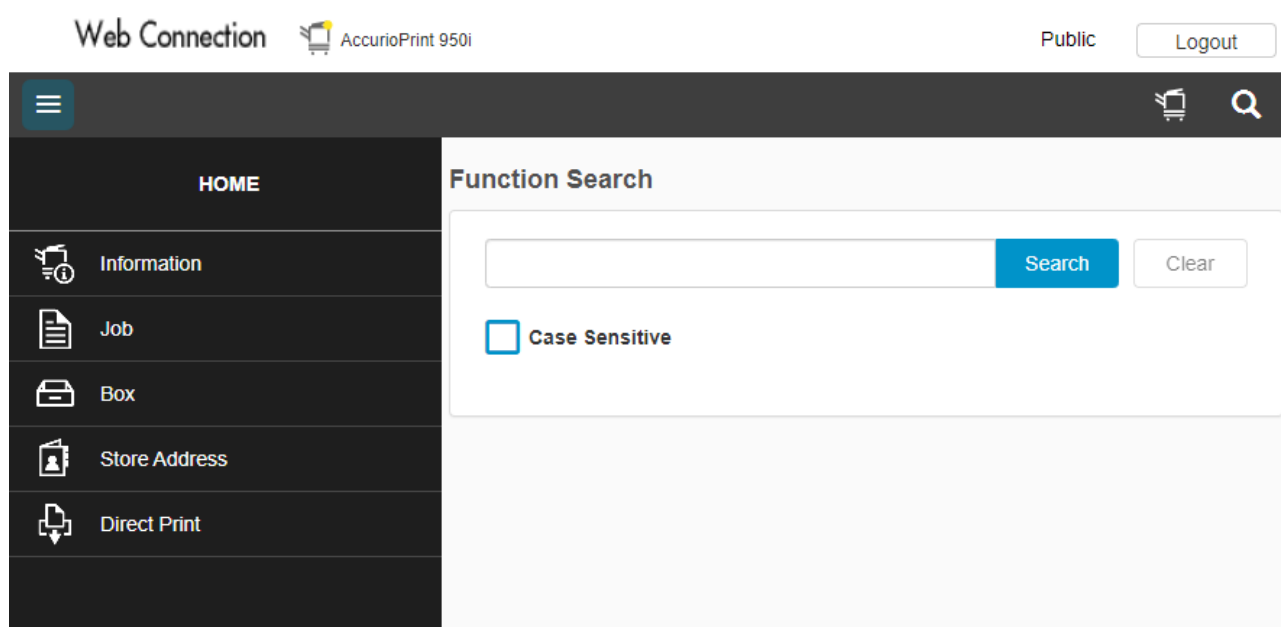
To protect against CVE-2023-29552, SLP should be disabled on all systems running on untrusted networks, like those directly connected to the Internet. If that is not possible, then firewalls should be configured to filter traffic on UDP and TCP port 427. This will prevent external attackers from accessing the SLP service.

As an additional defence layer, when the device is placed in an untrusted network, we strongly recommend to make sure that the default administrator password has been changed to a more secure complex password. This will ensure that any potential attacker will not be able to log into an exposed device to enable the vulnerable protocol.

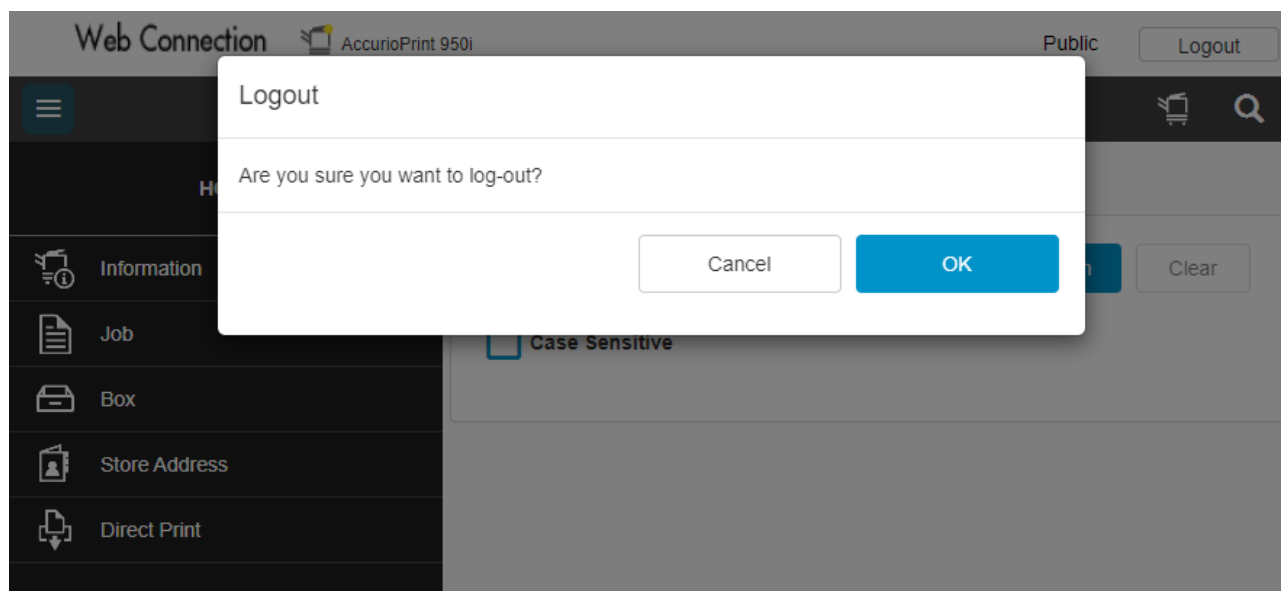
In our Office Printing and Production Printing devices, the "SLP Setting" can usually be configured via Network Settings within the Administrator mode. The setting can be accessed via the MFP panel, PageScope Web Connection or Remote Panel.

The following example is based on our IT6 Controller generation utilized in the i-Series lineup:


1. Firstly, access the device by entering the IP address in to your web browser.



2. Click on logout to exit the Public User mode.



- Next, select the Administrator as the User Type and enter the password.

Web Connection  AccurioPrint 950i

Please select a user type to login. EN

**Login**


User Type: Administrator

Password:

Data Management Utility

Starting-up Data Management Utility: Manage Copy Protect Data

- Once logged in, select Network.

Web Connection  AccurioPrint 950i Administrator

**HOME**

Administrator

Maintenance

System Settings

Security

User Auth/Account Track

**Network**

Box

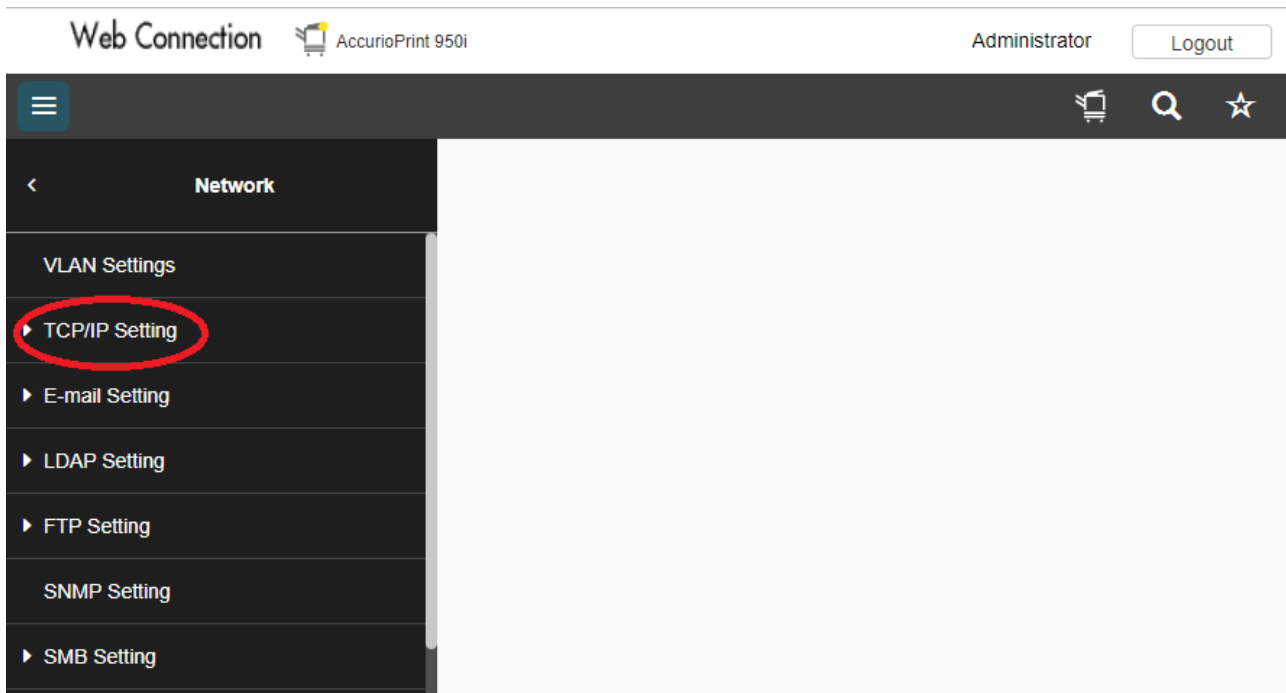
Printer Settings

**Function Search**

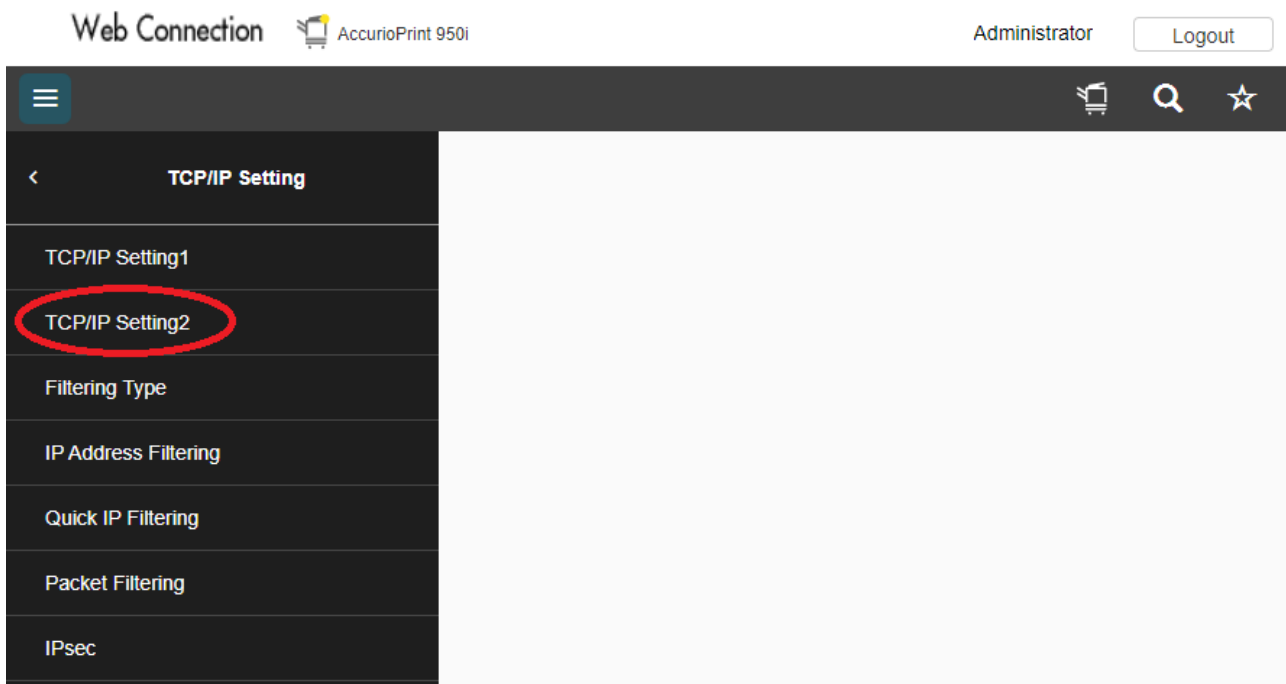
☐ Case Sensitive



5. Now select TCP/IP Setting.



6. Next, select TCP/IP Setting2.



7. Lastly, toggle the SLP setting switch to Off and press OK to save.

The screenshot shows the 'Web Connection' interface for an 'AccurioPrint 950i' device. The user is logged in as 'Administrator'. The left sidebar shows a menu with 'TCP/IP Setting' selected. The main area is titled 'TCP/IP Setting2' and contains the following settings:

RAW Port Number		
<input checked="" type="checkbox"/>	Port1	9100 (1-65535)
<input checked="" type="checkbox"/>	Port2	9112 (1-65535)
<input checked="" type="checkbox"/>	Port3	9113 (1-65535)
<input checked="" type="checkbox"/>	Port4	9114 (1-65535)
<input checked="" type="checkbox"/>	Port5	9115 (1-65535)
<input checked="" type="checkbox"/>	Port6	9116 (1-65535)

Below the ports, there is an 'SLP Setting' section with a toggle switch for 'SLP'. The switch is currently in the 'On' position (blue half visible) and is circled in red. At the bottom right, there are 'Cancel' and 'OK' buttons.

Alternatively, the SLP setting can be configured through fleet management solutions such as, Remote Deployment Tools (RDT) or FleetRMM. For more information, please contact your local Konica Minolta representative.

For other Konica Minolta devices and controller generations, please refer to the user guides available via:

- [Konica Minolta Online Manuals](#)
- [Konica Minolta Download Centre](#)



KONICA MINOLTA