KONICA MINOLTA

Open IPP Report – Exposed Printer Devices on the Internet

SECURITY WHITE PAPER

Table of Contents

Background

In June 2020, The SHADOWSERVER Foundation published a report which explains that their IPP (Internet Printing Protocol) scan uncovered approximately 80,000 open devices (printers) per day that were exposed to the Internet.

https://www.shadowserver.org/news/open-ipp-report-exposed-printer-devices-on-the-internet/

Device Access from the Internet

In order to make a printer or MFP (multifunctional printer) available on the Internet, it must be accessible via a public IP address.

There may be a small difference between using IPv4 or IPv6 IP addresses.

IP v4

Usually Internet providers only allocate one public IP address to the router, which then offers a local network with private IP addresses connection to the Internet. For direct access to the printer via IPP, the router needs to be configured to forward the IPP printing port to the dedicated printer's IP address.

Printers can be directly connected to the Internet. As an example, when configuring a printer directly to the modem, instead of connecting it to a router, the printer may be assigned a public IP address. Customers who have their own public IP address range, may use one of those IP addresses and assign one to the printer.

IP v6

With IPv6, the possibility of exposing the printer to the Internet is even higher.

One of the design principles of IPv6 is global reachability, which means except for the 'link local' IP addresses (fe80::), all IP addresses will be reachable over the Internet. However if a router is configured to distribute the public IPv6 range (by router advertisements), all locally connected devices may retrieve at least one IPv6 from that range. All locally connected devices may be accessible from the Internet if the router does not block incoming traffic.

Protect device from Access

A device can be accessed from the Internet, depending on the network and router configuration.

To secure the device the following measures are recommended:

- It is best practice to use local IP addresses only for the printer.
- If using a public IP address cannot be avoided, it is necessary to configure the firewall/router to block all incoming connections. Nowadays most routers have this set as default.
- Enable IPP authentication on the MFP.

In addition the following printer/MFP settings can mitigate the risk:

- Disable IPv6 to avoid accidental assignment of public IPv6 addresses.
- Use of IP address filtering will limit devices that can communicate with the printer.
- Enabling user authentication on the device will discard print jobs when incorrect authentication information is input.

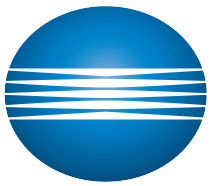
General Security Considerations

Konica Minolta products deploy a wide range of security related functions. The functionality may vary depending on the model.

Various security functions are largely taken into account when enabling the "Enhanced Security Mode" feature.

To assist our customers in securing their Konica Minolta device, we offer 'bizhub SECURE' which allows for different subsets of configurations.

In addition, customers may request individual consultancy in order to achieve a tailor-made product configuration.



KONICA MINOLTA

Konica Minolta South Africa, a division of Bidvest Office (Pty) Ltd
www.konicaminoltasa.com