PRODUCT BULLETIN

MPPB-129

INTERNAL USE ☒F ☐L

Date: 07/26/17	**Author:** Pete Kressin
Product: **LaserWash®** ☐ 4000 ☒ G5 ☒ M5 ☒ 360 Plus ☒AutoXpress™ | **ProTouch®** ☒ Tandem™ ☒ ICON™ | ☒ Access® ☐ MaxAir® ☒ LaserWash 360 ☒ LaserWash AutoXpress Plus	
Product Serial No: N/A	
Code: 4 - Possible field issues and may contain suggested corrective actions (informational).	
Subject: Network Security	

Recently, a security researcher made a presentation at a cybersecurity industry conference suggesting that there are potential issues with login security for the above-listed PDQ systems. PDQ is currently working on investigating and remediating any actual issues raised. Independently, PDQ has determined that improvements can be made to strengthen the software code that controls machine login security, and these improvements are under development and will be implemented on the next software revision for each product.

There are steps that every customer should take now to protect machines from unauthorized access. All systems—especially internet-connected ones—must be configured with security in mind. As a reminder for all sites with these machines installed, please take note of the following important things to have in place to ensure security from unauthorized access to the machine:

1) Always make sure any PDQ equipment noted above is not open to access from the internet; it should be behind a secure firewall.
2) Whenever a machine or router is received and installed, always change the default password from the factory settings to a new password unique to the machine. If an existing site is still using the factory default passwords on a machine or router, immediately change the default password to a new, unique, strong password.
3) Always set up the system network (router or Wi-Fi) with its security features enabled such that they require a username and password to be able to access the machine network.
4) Do not set up the site router with “port forwarding” enabled. This can effectively expose the system to the internet and may permit an unauthorized person to reach the machine login screen.
5) Do not share passwords or write them down in an accessible place where unauthorized users may find them.

For further information or help with specific cases, please contact PDQ Technical Support.

Parts and Assemblies:

Description	Part Number	QTY
N/A		