Release Notes: LW75.xx.P043

READ THIS FIRST: Special notes and considerations

- **Upgrade guidelines:**
  - This firmware release is intended for customers with current firmware versions LW73.xx.P034, LW72.xx.P030, LW71.xx.P025, LW70.xx.P022, or older (releases where the 2 digits immediately after LW are less than 70)
  - If the current firmware on the device is LW70.xx.P200 or newer (releases where the 3 digits after P are greater than 200), do NOT update to this release. Contact the Technical Support Center for a newer version of firmware.

- **Downgrading to EC4.0 or EC4.05:**
  - Due to changes in EC4.0 and EC5, do NOT downgrade firmware from EC5 or newer directly to EC4.0 or EC4.05 based code. EC4.0 and EC4.05 code levels have names like LW40.xx.P4xx. This will cause a non-clearable 900 Service error. Contact the TSC for instructions on how to clear this error.
  - This warning includes installing a DLE with EC4.0 or EC4.05 code into a device that currently has EC5 or newer code.
  - Code levels earlier than EC4.0 can be sent to EC5 level devices without causing a service error.
  - To downgrade EC5 or newer code to an EC4.0 or EC4.05 level, you must first load an EC4.1 based code. EC4.1 code levels have names like LW41.XX.P4xx. Once the device is at an EC4.1 level, EC4.0 code can be sent.
  - According to the firmware FAQ posted on the support site, we do not officially support downgrading firmware. This is the reason it is not supported, even though great efforts are made to prevent these kinds of events from happening, sometimes it is unavoidable. We apologize for the inconvenience.

CUSTOMER RELEASE NOTES:

Base firmware EC7.5, LW75.xx.P043, for the following devices (changes since EC6.3, LW63.xx.P638)

New features:

- Changes in LW75.xx.P043
  - Non-java remote op panel
  - Apps displaying "For testing purposes only. Not to be deployed to production" after FW update
  - Mopria recertification
  - CVE-2019-18791
  - CVE-2019-19773 – Fixed reflected XSS Vulnerability
  - CVE-2019-19772 – Fixed stored XSS Vulnerability
  - GDPR: Anonymous string appear under ISTL More Info screen

    - GDPR: User Information - Level setting appears under ISTL menu
    - ETL-Apps (Cloud 2.1): [SECURITY] – Removed info GUI debug data
    - Fixed Cross Site Scripting Issue
- Changes in LW72.xx.P030
    - etherFAX Support
        - ATTENTION: Setting the Fax Transport to 'etherFAX' will cause the fax feature to be unavailable unless the user has an active account for this device with etherFAX, LLC. You can contact etherFAX, LLC at www.etherfax.net, or call 1-877-384-9866 or 1-732-813-0990.
- Changes in LW70.xx.P022
    - Added SMBv3 support. See KB Article #FA1227 for more details
    - Enhanced TLS 1.2 support. Can now disable TLS 1.0 and TLS1.1
    - Added new "SSL Cipher List" setting
    - Updated openSSL to version 1.0.2j
    - Added support for PKCS #12 security certificates standard

Apps (eTask models only):

- Changes in LW74.xx.P037
    - Scan to Network app – v4.9.19
- Changes in LW73.xx.P034
    - Update Card Copy App to version 2.12.6 (fixes an issue with the app on 4.3” UI devices)
- Changes in LW70.xx.P022
    - EcoSettings app - v3.0.11 (4.3" op panels) and v3.5.9 (7" op panel)
    - Background and Idle Screen app - v3.11.0
    - Forms and Favorites app – v4.3.3 (for 7" & 10" op panels) and v3.3.3 (for 4.3" op panels)
    - Scan to Network app – v4.9.7
    - Card Copy app – v2.12.5
    - Multi Send app – v2.7.6
    - My Shortcut app – v1.6.1

Security Issues Addressed:

- Changes in LW74.xx.P037
    - Updated Java certificates for remote operator panel access
    - Security improvements based on internal testing
    - Added authenticated proxy support
- Changes in LW73.xx.P034
    - SNMP Denial of Service Vulnerability - CVE-2019-9931
    - Lexmark Overflow Vulnerabilities
        - CVE-2019-9930
        - CVE-2019-9932
        - CVE-2019-9933

  - Cross Site Request Forgery - CVE-2019-10057
  - Account Lockout - CVE-2019-10058
  - Information Disclosure via finger service - CVE-2019-10059
  - Information Disclosure Vulnerability
    - CVE-2019-9934
    - CVE-2019-9935
  - Shortcut Integrity vulnerability - CVE-2019-6489
- Changes in LW72.xx.P030
  - Directory Traversal Vulnerability - CVE-2018-18894
- Changes in LW71.xx.P025
  - Lexmark Buffer Overflow Vulnerability - CVE-2018-15519
- Changes in LW70.xx.P022
  - Addressed KRACK which has the following CVEs associated with it:
    - CVE-2017-13077
    - CVE-2017-13078
    - CVE-2017-13079
    - CVE-2017-13080
    - CVE-2017-13081
    - CVE-2017-13082
    - CVE-2017-13084
    - CVE-2017-13086
    - CVE-2017-13087
    - CVE-2017-13088

Field Issues Addressed and Other Improvements:

- Changes in LW74.xx.P037
  - Improvements to Scan to Network using SMBv3
  - Fix issue wtih clearing the restricted server list via MVE
  - Fix issue with printer not prompting for Universal media size when printing via IPP
  - Improve Cloud app deployment
- Changes in LW73.xx.P034
  - Fix for a 900.00 error when receiving a fax that contains a blank page when the Fax Transport is set to etherFAX
  - Fix to handle special XML characters in reporting
  - Translations changes
  - Improve capability for concurrent app presence
- Changes in LW71.xx.P025
  - Fixed issue where an App crashes when sanitizing edit box using single quotes in their VLML
  - Removed anonymous authentication ciphers from factory default values
  - Fixed crash when shutting down SMB
- Changes in LW70.xx.P022

- Update jar signing algorithm for Remote Operator Panel and Scan Profile java applets
- Fix for an issue where PDF scans with 1-bit mono images were unreadable by iOS10 and up
- Fix for an issue on MX31x devices where pressing the sleep button does not put the device to sleep even when the setting is configured to do so
- Fixes for several 900.xx crashes
- Multiple fixes for blank screen, white screen, and busy screen hangs
- Multiple translations changes
- Multiple card reader fixes
- Multiple fixes for PDF, PS, and PCL print job errors
- Multiple fixes for fax and fax-over-IP

Supported Models:

Model	Firmware Version
Mono Single Function Devices	
MS310d, MS310dn (LED)	LW75.PRL.P043
MS312dn, MS317 (2-Line)	LW75.PRL.P043
MS315dn (2.4”)	LW75.TL2.P043
MS410d, MS410dn (2-Line)	LW75.PRL.P043
MS415dn, MS417 (2.4”)	LW75.TL2.P043
MS51x Series, MS610dn, MS617 (2.4”)	LW75.PR2.P043
MS610de (4.3” eTask)	LW75.PR4.P043
MS71x Series (2.4”)	LW75.DN2.P043
MS810, MS811, MS812, MS817, MS818 (2.4”)	LW75.DN2.P043
MS810de (4.3” eTask)	LW75.DN4.P043
MS812de (4.3” eTask)	LW75.DN7.P043
MS91x Series (4.3” eTask)	LW75.SA.P043
Mono Multi Function Devices	
MX31x Series (2.4”)	LW75.SB2.P043

MX41x Series, MX51x Series (4.3” eTask)	LW75.SB4.P043
MX61x Series (7.0” eTask)	LW75.SB7.P043
MX71x Series, MX81x Series (7.0”/10.0” eTask)	LW75.TU.P043
MX91x Series (10” eTask)	LW75.MG.P043
MX6500e	LW75.JD.P043
Color Single Function Devices	
CS31x Series (2-Line)	LW75.VYL.P043
CS41x Series (2.4”)	LW75.VY2.P043
CS51x Series (4.3” eTask)	LW75.VY4.P043
Color Multi Function Devices	
CX31x Series (2.4”)	LW75.GM2.P043
CX41x Series (4.3” eTask)	LW75.GM4.P043
CX51x Series (7.0” eTask)	LW75.GM7.P043