```
==============================================================================
*** Basic Information ***
==============================================================================
[Create date] 2019/12/20
----------------------------------------------------------------------
[Program Name] Main
----------------------------------------------------------------------
[Version] 1.13
----------------------------------------------------------------------
[PCB No.]
----------------------------------------------------------------------
[Interchangeability] X / O
----------------------------------------------------------------------
[Other Firmware Requirements] None
----------------------------------------------------------------------
[PCB Requirements] None
----------------------------------------------------------------------
[Software category] Normal Release
----------------------------------------------------------------------
[Release category] Normal Release
----------------------------------------------------------------------
[Program category] Firmware
----------------------------------------------------------------------
Exported to(language) GEN(all)
[Firmware No.] M1565051K
[File Information]
 File Name        M1565051K.zip
 File Type        Module for Service
 Size             6.28 MB ( 6584886 byte )
[Availability of RFU] No
----------------------------------------------------------------------
[Production reflection]
----------------------------------------------------------------------

==============================================================================
*** Note ***
==============================================================================
[Note]

----------------------------------------------------------------------


==============================================================================
*** Important Notes ***
==============================================================================
[Important Notes]

----------------------------------------------------------------------


==============================================================================
*** Modification History ***
==============================================================================
[Modifications made:]
Rank C
```

Symptom corrected:
- A vulnerability (CVE-2019-14302) to allowing access to memory data
  via the UART port has been fixed.
- A vulnerability (CVE-2019-14301) to unauthenticated access to the
  debug page in the Web Image Monitor has been fixed.
- A vulnerability (CVE-2019-14304) to Cross-Site Request Forgery in
  the Web Image Monitor has been fixed.
- A vulnerability (CVE-2019-14306) to unauthenticated access to
  backup files in the Web Image Monitor has been fixed.
- A vulnerability (CVE-2019-14300) to buffer overflows parsing HTTP
  cookie headers has been fixed.
- A vulnerability (CVE-2019-14305) to buffer overflows in some
  setting values has been fixed.
- A vulnerability (CVE-2019-14307) to a denial of service attack on
  setting SMTP values has been fixed.
- A vulnerability (CVE-2019-14308) to a potential buffer overflow
  sending a crafted LPD packet has been fixed.

[Modification history]

Version 1.12
Rank C

Other changes:
- The Scan to Folder function is available on Mac OS X 10.13 because
  SMBv2 is now supported.

Version 1.11
System corrected:
- A minor bug fix of the fax function.
- The CIS in the scanner unit was modified in line with the bug fix.
- When "DHCP" is set to "Active" and "DNS Method" is set to "Auto-
  Obtain (DHCP)", an extra character is added in the domain name.

Version 1.10
Symptom corrected:
1. Scan to E-Mail does not work.
2. Abnormal noise is generated while sending a FAX.
3. Cannot send Hostname to the DHCP server via DHCP Option55, Option12.
4. Talking on the handset while set to FAX/Answering machine causes
   to switch to the FAX mode.
5. "Total No. of Rings (TAD)" was missing from the Reception Setting Menu.
6. Minor bug fixed.

Version 1.09
Changed: Minor bug correction.

Version 1.08
Specification change:

1. Traditional Chinese has been supported.

Symptom corrected:

2. The XSS vulnerability on Web Image Monitor.
3. The FAX communication between two SP 310SFN, or SP 311SFN in ECM mode will cost unexpected long time.

Version 1.06
Other changes:
Supports the new model (SP312SFNw) released for the China market.

Symptom corrected:

1. If Scan to FTP tries to access a nonexistent server more than four times, the function will not work until the device undergoes a power cycle.
2. The gateway address might be cleared when its lease from the DHCP server expires, which would cause the related connections to other segments to fail.

Version 1.04
1st Mass production

```
================================================================================
*** Basic Information ***
================================================================================
[Create date] 2019/12/24
------------------------------------------------------------------------
[Program Name] Main
------------------------------------------------------------------------
[Version] 1.06
------------------------------------------------------------------------
[PCB No.]
------------------------------------------------------------------------
[Interchangeability] X / O
------------------------------------------------------------------------
[Other Firmware Requirements] None
------------------------------------------------------------------------
[PCB Requirements] None
------------------------------------------------------------------------
[Software category] Normal Release
------------------------------------------------------------------------
[Release category] Normal Release
------------------------------------------------------------------------
[Program category] Firmware
------------------------------------------------------------------------
Exported to(language) GEN(all)
[Firmware No.] M2925051D
[File Information]
 File Name        M2925051D.zip
 File Type        Module for Service
 Size             5.23 MB ( 5481773 byte )
[Availability of RFU] No
------------------------------------------------------------------------
[Production reflection]
------------------------------------------------------------------------

================================================================================
*** Note ***
================================================================================
[Note]

------------------------------------------------------------------------



================================================================================
*** Important Notes ***
================================================================================
[Important Notes]

------------------------------------------------------------------------



================================================================================
*** Modification History ***
================================================================================
[Modifications made:]
Rank C
```

Symptom corrected:

- A vulnerability (CVE-2019-14302) to allowing access to memory data via the UART port has been fixed.
- A vulnerability (CVE-2019-14301) to unauthenticated access to the debug page in the Web Image Monitor has been fixed.
- A vulnerability (CVE-2019-14304) to Cross-Site Request Forgery in the Web Image Monitor has been fixed.
- A vulnerability (CVE-2019-14306) to unauthenticated access to backup files in the Web Image Monitor has been fixed.
- A vulnerability (CVE-2019-14300) to buffer overflows parsing HTTP cookie headers has been fixed.
- A vulnerability (CVE-2019-14305) to buffer overflows in some setting values has been fixed.
- A vulnerability (CVE-2019-14307) to a denial of service attack on setting SMTP values has been fixed.
- A vulnerability (CVE-2019-14308) to a potential buffer overflow sending a crafted LPD packet has been fixed.

[Modification history]

Version 1.05
Symptom corrected:
When "DHCP" is set to "Active" and "DNS Method" is set to "Auto-Obtain (DHCP)", an extra character is added in the domain name.

Version 1.04
System corrected:
- Cannot use the AIO, if the engine memory had been cleared in the SP mode.
See RTB RM292005a for detail.

Version 1.03
Symptom corrected:
The printer sends counter and supply information to PaaS server every 3 seconds. (Normal communication between the printer and PaaS server should be once a day.)

```
========================================================================
*** Basic Information ***
========================================================================
[Create date] 2019/12/24
------------------------------------------------------------------------
[Program Name] Main
------------------------------------------------------------------------
[Version] 1.10
------------------------------------------------------------------------
[PCB No.]
------------------------------------------------------------------------
[Interchangeability] X / O
------------------------------------------------------------------------
[Other Firmware Requirements] None
------------------------------------------------------------------------
[PCB Requirements] None
------------------------------------------------------------------------
[Software category] Normal Release
------------------------------------------------------------------------
[Release category] Normal Release
------------------------------------------------------------------------
[Program category] Firmware
------------------------------------------------------------------------
Exported to(language) GEN(all)
[Firmware No.] M2935051G
[File Information]
 File Name        M2935051G.zip
 File Type        Module for Service
 Size             5.37 MB ( 5635541 byte )
[Availability of RFU] No
------------------------------------------------------------------------
[Production reflection]
------------------------------------------------------------------------

========================================================================
*** Note ***
========================================================================
[Note]

------------------------------------------------------------------------



========================================================================
*** Important Notes ***
========================================================================
[Important Notes]

------------------------------------------------------------------------



========================================================================
*** Modification History ***
========================================================================
[Modifications made:]
Rank C
```

Symptom corrected:

- A vulnerability (CVE-2019-14302) to allowing access to memory data via the UART port has been fixed.
- A vulnerability (CVE-2019-14301) to unauthenticated access to the debug page in the Web Image Monitor has been fixed.
- A vulnerability (CVE-2019-14304) to Cross-Site Request Forgery in the Web Image Monitor has been fixed.
- A vulnerability (CVE-2019-14306) to unauthenticated access to backup files in the Web Image Monitor has been fixed.
- A vulnerability (CVE-2019-14300) to buffer overflows parsing HTTP cookie headers has been fixed.
- A vulnerability (CVE-2019-14305) to buffer overflows in some setting values has been fixed.
- A vulnerability (CVE-2019-14307) to a denial of service attack on setting SMTP values has been fixed.
- A vulnerability (CVE-2019-14308) to a potential buffer overflow sending a crafted LPD packet has been fixed.

[Modification history]

Version 1.08
Symptom corrected

- The daily communication with the PaaS server using a 3G dongle cannot inform counter and supply information.
- After the daily communication with the PaaS server using a 3G dongle, the device cannot communicate with client computers in other segments in an ethernet (wired LAN) environment.

Version 1.06
Symptom corrected:
When "DHCP" is set to "Active" and "DNS Method" is set to "Auto-Obtain (DHCP)", an extra character is added in the domain name.

Version 1.05
Symptom corrected:

- Supported machines for India.

Version 1.04
Symptom corrected:
Image background might get dirty when printing in low temperature and low humidity environment.

Version 1.03
1st Mass production

```
========================================================================
*** Basic Information ***
========================================================================
[Create date] 2019/12/24
------------------------------------------------------------------------
[Program Name] Main
------------------------------------------------------------------------
[Version] 1.06
------------------------------------------------------------------------
[PCB No.]
------------------------------------------------------------------------
[Interchangeability] X / O
------------------------------------------------------------------------
[Other Firmware Requirements] None
------------------------------------------------------------------------
[PCB Requirements] None
------------------------------------------------------------------------
[Software category] Normal Release
------------------------------------------------------------------------
[Release category] Normal Release
------------------------------------------------------------------------
[Program category] Firmware
------------------------------------------------------------------------
Exported to(language) GEN(all)
[Firmware No.] M2945051C
[File Information]
 File Name         M2945051C.zip
 File Type         Module for Service
 Size              6.74 MB ( 7062323 byte )
[Availability of RFU] No
------------------------------------------------------------------------
[Production reflection]
------------------------------------------------------------------------

========================================================================
*** Note ***
========================================================================
[Note]

------------------------------------------------------------------------



========================================================================
*** Important Notes ***
========================================================================
[Important Notes]

------------------------------------------------------------------------



========================================================================
*** Modification History ***
========================================================================
[Modifications made:]
Rank C
```

Symptom corrected:
- A vulnerability (CVE-2019-14302) to allowing access to memory data via the UART port has been fixed.
- A vulnerability (CVE-2019-14301) to unauthenticated access to the debug page in the Web Image Monitor has been fixed.
- A vulnerability (CVE-2019-14304) to Cross-Site Request Forgery in the Web Image Monitor has been fixed.
- A vulnerability (CVE-2019-14306) to unauthenticated access to backup files in the Web Image Monitor has been fixed.
- A vulnerability (CVE-2019-14300) to buffer overflows parsing HTTP cookie headers has been fixed.
- A vulnerability (CVE-2019-14305) to buffer overflows in some setting values has been fixed.
- A vulnerability (CVE-2019-14307) to a denial of service attack on setting SMTP values has been fixed.
- A vulnerability (CVE-2019-14308) to a potential buffer overflow sending a crafted LPD packet has been fixed.

[Modification history]

Version 1.05
System corrected:
- A minor bug fix of the fax function.
- The CIS in the scanner unit was modified in line with the bug fix.
- When "DHCP" is set to "Active" and "DNS Method" is set to "Auto-Obtain (DHCP)", an extra character is added in the domain name.

Version 1.04
System corrected:
- Cannot use the AIO, if the engine memory had been cleared in the SP mode.

See RTB RM292005a for detail.

```
================================================================================
*** Basic Information ***
================================================================================
[Create date] 2019/12/24
------------------------------------------------------------------------
[Program Name] Main
------------------------------------------------------------------------
[Version] 1.10
------------------------------------------------------------------------
[PCB No.]
------------------------------------------------------------------------
[Interchangeability] X / O
------------------------------------------------------------------------
[Other Firmware Requirements] None
------------------------------------------------------------------------
[PCB Requirements] None
------------------------------------------------------------------------
[Software category] Normal Release
------------------------------------------------------------------------
[Release category] Normal Release
------------------------------------------------------------------------
[Program category] Firmware
------------------------------------------------------------------------
Exported to(language) GEN(all)
[Firmware No.] M2955051G
[File Information]
 File Name         M2955051G.zip
 File Type         Module for Service
 Size              6.95 MB ( 7291502 byte )
[Availability of RFU] No
------------------------------------------------------------------------
[Production reflection]
------------------------------------------------------------------------

================================================================================
*** Note ***
================================================================================
[Note]

------------------------------------------------------------------------



================================================================================
*** Important Notes ***
================================================================================
[Important Notes]

------------------------------------------------------------------------



================================================================================
*** Modification History ***
================================================================================
[Modifications made:]
Rank C
```

Symptom corrected:
- A vulnerability (CVE-2019-14302) to allowing access to memory data via the UART port has been fixed.
- A vulnerability (CVE-2019-14301) to unauthenticated access to the debug page in the Web Image Monitor has been fixed.
- A vulnerability (CVE-2019-14304) to Cross-Site Request Forgery in the Web Image Monitor has been fixed.
- A vulnerability (CVE-2019-14306) to unauthenticated access to backup files in the Web Image Monitor has been fixed.
- A vulnerability (CVE-2019-14300) to buffer overflows parsing HTTP cookie headers has been fixed.
- A vulnerability (CVE-2019-14305) to buffer overflows in some setting values has been fixed.
- A vulnerability (CVE-2019-14307) to a denial of service attack on setting SMTP values has been fixed.
- A vulnerability (CVE-2019-14308) to a potential buffer overflow sending a crafted LPD packet has been fixed.

[Modification history]

Version 1.09
Rank C

Other changes:
- The Scan to Folder function is available on Mac OS X 10.13 because SMBv2 is now supported.

Version 1.08
Symptom corrected
- The daily communication with the PaaS server using a 3G dongle cannot inform counter and supply information.
- After the daily communication with the PaaS server using a 3G dongle, the device cannot communicate with client computers in other segments in an ethernet (wired LAN) environment.

Version 1.06
System corrected:
- A minor bug fix of the fax function.
- The CIS in the scanner unit was modified in line with the bug fix.
- When "DHCP" is set to "Active" and "DNS Method" is set to "Auto-Obtain (DHCP)", an extra character is added in the domain name.

Version 1.05
Symptom corrected:
- Supported machines for India.

Version 1.04

Symptom corrected:
Image background might get dirty when printing in low temperature
and low humidity environment.

Version 1.02
1st Mass production