

=====
*** Basic Information ***
=====

[Create date] 2019/10/31

[Program Name] GDI

[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.] D2455503H

[File Information]

File Name D2455503H.exe

File Type Module for Service

Size 4.58 MB (4798363 byte)

Check Sum -8Bit Sum: AB9F

 -16Bit Sum(Little Endian): 477E

 -16Bit Sum(Big Endian): 0321

[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.

[Modification history]

Version 1.09

Symptom Corrected:

1. If [DHCP] is set to "Active" and [DNS Method] to "Auto-Obtain (DHCP)," an extra character is added to the domain name.

Modification:

1. Default setting of PM parts replacement notice display

The default setting of PM parts replacement notice was changed to not display, as this information should appear only when set by the CE.

2. Translation correction (China Only)

Toner replacement => (Corrected to) PCPU replacement

Version 1.08

Specification Change:

1. Margin was increased to prevent unwanted lines that may appear when copied with the ID Card Copy function.
2. Sort function added for the copy mode.
3. The default orientation of the original in duplex jobs was changed to "Always specified."
4. The default values of the following SP were changed for higher productivity in A4SEF jobs by preventing the hot roller from overheating.
SP1-124-007 (75 => 50)
SP1-124-008 (50 => 10)

Note: For example, if the job consists of 40 pages in A4SEF or FS (Legal size), copying stops for a while (at around the 14th page) and then resumes.

Version 1.07

Specification Change:

Reading range of the ID Card Copy was extended for improved performance.

Version 1.06

Symptom corrected:

- Jam may occur in duplex printing, if the paper is smaller than the image.

Version 1.05

Symptom corrected:

A Scan Forwarding job cannot be cancelled with the [Stop] key if the original is being scanned on the exposure glass.

The LCD backlight does not turn on when the toner bottle is replaced.

Version 1.04

Symptom corrected:

1. "R & Dup U Cvr" or "R&T2R&T3R Cvr" may be displayed when a paper jam occurs.
2. A Copy job where the original is scanned on the exposure glass cannot be competed using the "#" key following a Folder Print job.
3. The machine freezes if the [Stop] key is pressed during a Copy job where the original is scanned on the exposure glass.

=====
*** Basic Information ***
=====

[Create date] 2019/11/06

[Program Name] GDI NIC

[Version] 2.04

[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.] D2455505C

[File Information]

File Name D2455505C.exe

File Type Module for Service

Size 5.14 MB (5389753 byte)

Check Sum -8Bit Sum: 31B7

 -16Bit Sum(Little Endian): 3CA4

 -16Bit Sum(Big Endian): AC13

[Availability of RFU] No

[Production reflection]

=====
*** Note ***
=====

[Note]

=====
*** Important Notes ***
=====

[Important Notes]

=====
*** Modification History ***
=====

[Modifications made:]

Rank C

Symptom corrected:

- A vulnerability (CVE-2019-14300) to buffer overflows parsing HTTP cookie headers 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-2019-14302) to allowing access to memory data via the UART port has been fixed.
- A vulnerability (CVE-2019-14304) to Cross-Site Request Forgery in the Web Image Monitor has been fixed.
- A vulnerability (CVE-2019-14305) to buffer overflows in some setting values 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-2019-14307) 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 2.03

Rank C

Other changes:

- The PaaS setting values will not change even if the machine reset by using the Factory Defaults menu in the SP mode.

Version 2.02

Rank C

Other changes:

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

Version 2.01

Rank C

Symptom corrected:

- The machine does not recover from the energy saving mode, if any key is pressed on the operation panel.
- When "DHCP" is set to "Active" and "DNS Method" is set to "Auto-Obtain (DHCP)", an extra character is added in the domain name.

Other changes:

- Supported PaaS for China.

