Driver vulnerability ‘How to’ guide

This document is a guide relating to the security fix issued to address potential vulnerabilities in some of Ricoh’s printer/PC fax drivers (see announcement here).

Version: 1.2
Date: 19th February 2020

Scope

Ricoh released an updated printer driver and security software to address the following privilege escalation vulnerability (CVE-2019-19363) which may affect some versions of the printer/PC fax drivers used by certain Ricoh MFPs, Printers and Digital Duplicators:

A DLL file in a printer driver folder can be replaced by users without administrator privileges. If the DLL was replaced, a malicious attacker could operate the driver and/or the PC or Server with higher privileges.

Affected drivers: https://www.ricoh.com/info/2020/0122_1/list
Operating Systems: All supported Windows versions

Applying the Printer Driver Security Program Ver.1.3.0.0

The Security Program file “PrinterFAXDriverSecurityProgram.msi” can be downloaded from the Ricoh download page:
http://support.ricoh.com/bb/html/dr_ut_e/re1/model/Security_Patch/Security_Patch.htm

Notes:

- *Please make sure to use the correct “PrinterFAXDriverSecurityProgram.msi” file, as any previous versions will not secure/patch the driver.*
- *The Security Program is available only in English, but it supports non-English environment.*

This file must be executed on any Windows-based PC or Server that has affected Ricoh printer drivers installed. This includes both print servers and any clients.

Note: The Security Program is not distributed by the Point and Print mechanism.

Restart the PC or Server prior to applying the Security Program. For the Security Program to work the file must run with administrator privileges.

The Security Program will display a “Installation Complete” message box after successful application. If unsuccessful, restart the PC or Server and apply the Security Program again.

Restarting the PC or Server after applying the Security Program is strongly recommended.

The Security Program will work for all affected drivers at once.

Note: If you install an affected driver after the Security Program was already installed, you must re-run the Security Program to fix the new driver.

How the Security Program works

Basically, what the Security Program patch will do is to change the access permissions of "RICOH_DRV", "RICOH" and their subfolders/files.

Location of the "RICOH_DRV" and "RICOH" folders:
C:\ProgramData\RICOH_DRV
C:\ProgramData\RICOH

Notes:

- *"*ProgramData", "RICOH_DRV" and "RICOH" are hidden folders.
- *Depending on the installed drivers, "RICOH_DRV" or "RICOH" do not exist on the PC or Server.*

However, before changing the permissions, the patch will do the following per printer driver:

- Unzip a *.dlz file (zipped DLL files) in the Windows "3" folder and compare the unzipped *.dll files with *.dll files in the "dlz" folder in "C:\ProgramData\RICOH_DRV*printer driver name*_common" or "C:\ProgramData\RICOH *printer driver name*_common".

  Location of the "3" folder:
  64-bit driver: C:\Windows\System32\spool\drivers\x64\3
  32-bit driver: C:\Windows\System32\spool\drivers\W32X86\3
- When the *.dll files are the same, the patch will just change the permissions. If not, the patch will overwrite the *.dll files in the *.dlz folder with the unzipped *.dll files, then change the permissions.

The reason for this behaviour is that when a driver is updated, not all new *.dll files overwrite old *.dll files in the 'dlz' folder at once. Some *.dll files in the 'dlz' folder are updated when a user has opened the driver UI or has printed.

If access permissions have been changed before old *.dll files are updated, the *.dll files will never be updated with user privileges. To prevent this, the patch makes sure that *.dll files in the 'dlz' folder are not old ones.

Alternative to Security Program all installed drivers

The new versions of PCL6 Driver for Universal Print 4.27 and PS Driver for Universal Print 4.27 include a silent version of this Security Program. So, if you install this driver (anticipated to be available on 11 March 2020), the Security Program will run during installation and will Security Program all Ricoh drivers on the target PC or Server.

You can download the drivers here:
http://support.ricoh.com/bb/html/dr_ut_e/rc3/model/p_i/p_i.htm?lang=en

PCL6/PS Driver for Universal Print version 4.27

Version 4.27 of the Universal Print Drivers is patched as the driver package contains a silent version of PrinterFAXDriverSecurityProgram.msi. (NB Version 4.27 of the UPD is expected to be released on 11 March 2020).

Note: Please do not use version 4.25 of the Universal Print Driver – which was available for a short time around the end of 2019.

20 Triton Street, London, NW1 3BF. Phone: +44 (0) 207 465 1153
E-mail : media@ricoh-europe.com

Version 4.26 and prior are not patched. We recommend updating/patching these drivers as soon as possible. This will also patch any device-specific drivers you might have installed on the target PC or Server.

Note: The user interface of version 4.26 onwards has changed to reflect the latest customer feedback.

Q&A

1. **Q) Will versioned drivers e.g. for the PCL6 Driver for Universal Print and PS Driver for Universal Print also be patched?**
   A) Yes.

2. **Q) When a new print queue has been created, should I run the Security Program again?**
   A) No, as long as an affected driver has not been installed/updated, running the Security Program again is not necessary. The Security Program will fix the vulnerability per installed driver, not per print queue.

3. **Q) Do I need to Security Program all servers and all clients?**
   A) Yes. The effect of PrinterFAXDriverSecurityProgram.msi will not be distributed to clients. However, in case PCL6/PS Driver for Universal Print 4.27 has been installed on a server, the silent version of the Security Program will be distributed (along with driver files) too and run on the clients when they connect to a print queue using the v.4.27 driver.

4. **Q) Can I identify if a PC or Server was already patched and if drivers are still vulnerable?**
   A) You can tell that the Security Program has been successfully applied if the access rights are set as below.

"C:\ProgramData\RICOH_DRV*printer driver name*_common\dlz" and
"C:\ProgramData\RICOH *printer driver name*_common\dlz":

Group or usernames	**Access rights**
SYSTEM	Full control
Administrators	Full control
Authenticated Users	Allow: Read and execute, List folder contents, Read
Users	Allow: Read and execute, List folder contents, Read

"RICOH_DRV", "RICOH", "*printer driver name*" and "_common" folders:

Group or usernames	**Access rights**
SYSTEM	Full control
Administrators	Full control

20 Triton Street, London, NW1 3BF. Phone: +44 (0) 207 465 1153
E-mail : media@ricoh-europe.com

Authenticated Users	Allow: Modify, Read and execute, List folder contents, Read, Write Deny: Delete (“This folder only”)
Users	Allow: Modify, Read and execute, List folder contents, Read, Write Deny: Delete (“This folder only”)

Notes:

- *Some of the folders mentioned above are hidden folders.*
- *Depending on the installed drivers, “RICOH_DRV” or “RICOH” do not exist on the PC or Server.*
- *“Everyone” should be removed from the list of Group or usernames.*
- *Manually changing the access rights can cause printing issues so make sure to use the Security Program or install PCL6/PS Driver for Universal Print version 4.27.*

5. Q) Will Ricoh release patched device-specific drivers?

A) Yes, but the schedule and target models are not finalised yet. In the meantime, please install the existing driver and apply the Security Program as of now.

6. Q) How can I check if the patch is installed and which version?

A) The latest version of the patch is v1.3.0. You can confirm installation and version of the patch in the Windows Control Panel (Control Panel\Programs\Programs and Features). Left click on the “Printer Fax Driver Security Program” to check the version.

7. Q) Are non-Ricoh drivers affected e.g. EFI Fiery controllers sold by Ricoh?

A) No, the Security Program only applies to Ricoh printer drivers.

8. Q) Can the security program be uninstalled?

A) Yes, it can be done via Windows “Programs and Features” by uninstalling "Printer FAX Driver Security Program". However, it will not deactivate the effect of the program (Access permissions will not be changed.) To release the security status, uninstall all Ricoh drivers and then install them again.

9. Q) Do I need to update the drivers even after running the Security Program?

A) Yes. The patch only addresses this vulnerability, while driver updates may contain additional updates or fixes. Downloading and installing the latest driver versions is recommended always as it is best practice to have the latest version installed to ensure optimal performance and security.

-ENDS-

20 Triton Street, London, NW1 3BF. Phone: +44 (0) 207 465 1153
E-mail : media@ricoh-europe.com