Title:	**Carestream Product Security Advisory – Print Nightmare**
Advisory ID:	CARESTREAM-2021-05
Issue Date:	07/15/2021
Last Revision Date:	01/05/2022
Revision #:	5

Vulnerability Summary:

Print Nightmare is a series of vulnerabilities in the Print Spooler service in all Microsoft Operating Systems that may be exploited to provide remote code execution on the target system.

CVE(s):

ID	CVSS	Released	Link
CVE-2021-1675	7.8	06/08/2021	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1675
CVE-2021-34527	9.8	07/16/2021	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
CVE-2021-34481	8.8	08/10/2021	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481
CVE-2021-36936	8.8	08/10/2021	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36936
CVE-2021-36947	8.8	08/10/2021	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36947

Additional Information:

- https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/printnightmare-critical-windows-print-spooler-vulnerability

Affected Products and Patch Availability:

Impacted by Vulnerability	Product	Patch Availability
ImageView V1.8-1.X Systems – Windows 10 IoT Enterprise 2019 LTSC		
Not impacted as Print Spooler service is disabled by default.	DRX-Evolution	Although not impacted, all Microsoft patches are qualified and released for ImageView systems every other month. See below for more information.
	DRX-Evolution Plus	
	DRX-Ascend	
	Q-Rad Systems	
	DRX Compass	
	DRX-1 System	
	DRX-Revolution	
	DRX-Revolution Nano	
	DRX-Mobile Retrofit	
	DRX Mobile Upgrade Solutions	
	DRX Mobile Upgrade Solutions	
	DRX-Transportable	
	DRX-Transportable Lite	
ImageView V1.2-1.7 Systems – Windows 10 IoT Enterprise 2016 LTSB		
Not impacted as Print Spooler service is disabled by default.	DRX-Evolution	Although not impacted, all Microsoft patches are qualified and released for ImageView systems every other month. See below for more information.
	DRX-Evolution Plus	
	DRX-Ascend	
	Q-Rad Systems	
	DRX Compass	
	DRX-1 System	
	DRX-Revolution	
	DRX-Revolution Nano	
	DRX-Mobile Retrofit	
	DRX Mobile Upgrade Solutions	
	DRX Mobile Upgrade Solutions	
	DRX-Transportable	
	DRX-Transportable Lite	
ImageView V1.1 Systems – Windows 10 IoT Enterprise 2016 LTSB		
Not impacted as Print Spooler service is disabled by default.	OnSight 3D Extremity System	Although not impacted, all Microsoft patches are qualified and released for ImageView systems every other month. See below for more information.
DirectView V5.7 Systems – Windows Embedded Standard 7 Service Pack 1		
Versions V5.7E and earlier are impacted.	CR975	All systems V5.7F or later and any system that has received a security update
	DIRECTVIEW Max CR System	
	DIRECTVIEW Classic CR System	

Impacted by Vulnerability	Product	Patch Availability
Versions V5.7F and later not impacted as Print Spooler service is disabled by default.	DIRECTVIEW Elite CR System	since June 2017 will have the Print Spooler service disabled as a preventative measure. For V5.7E and earlier systems, the latest qualified security update should be applied to disable the Print Spooler service. See below for more information.
	DirectView Remote Operations Panel	
	DRX-Evolution	
	DRX-Evolution Plus	
	DRX-Ascend	
	Q-Rad Systems	
	DRX Compass	
	DRX-1 System	
	DRX-Revolution	
	DRX-Revolution Nano	
	DRX-Mobile Retrofit	
	DRX Mobile Upgrade Solutions	
	DRX Mobile Upgrade Solutions	
	DRX-Transportable	
	DRX-Transportable Lite	
DirectView V5.2 – V5.6 Systems – Windows XP Embedded Service Pack 3		
Impacted	CR825	Carestream recommends installing the latest qualified security update which will disable the Print Spooler service. See below for more information.
	CR850	
	CR950	
	CR975	
	DIRECTVIEW Max CR System	
	DIRECTVIEW Classic CR System	
	DIRECTVIEW Elite CR System	
	DIRECTVIEW Remote Operations Panel	
	DR 3000	
	DR 3500	
	DR 7500	
	DR 9500	
	DRX-Evolution	
	DRX-Ascend	
	DRX-Innovation	
	Q-Rad Systems	
	DRX-1 System	
	DRX-Revolution	
	DRX-Mobile Retrofit	
	DRX-Neo	
	DRX Mobile Upgrade Solutions	
	DRX-Transportable	

Impacted by Vulnerability	Product	Patch Availability
	DRX-Transportable Lite	
Image Suite V4 Systems – Windows 10 Professional		
Impacted	CRescendo Classic Image Suite	Patch qualification completed. See below for more information.
	CRescendo WAIV Series with Touch Screen	
	CRescendo Vita Image Suite	
	CRescendo Max	
	Vita CR System	
	Vita Flex CR System	
	DRive	
	PRO Detector Systems	
Image Suite V4 Systems – Windows 8.1 Professional		
Impacted	CRescendo Classic Image Suite	Patch qualification completed. See below for more information.
	CRescendo WAIV Series with Touch Screen	
	CRescendo Vita Image Suite	
	CRescendo Max	
	Vita CR System	
	Vita Flex CR System	
	DRive	
	PRO Detector Systems	
Duet Version 1.0 – 1.13 – Windows Embedded Standard 7 Service Pack 1		
Impacted	DRX-Excel	Mitigations available. See below for more information
	DRX-Excel Plus	
Duet Version 1.20 – Windows 10 IoT Enterprise 2016 LTSB		
Impacted	DRX-Excel	Mitigations available. See below for more information
	DRX-Excel Plus	
OMNI Products		
Impacted	OMNI	Customers may self-patch Omni products. See below for more information.
X-Ray Detectors		
Not impacted	DRX Detectors	None
	DRX 2530C Detector	
	DRX Plus Detectors	
	DRX Plus 2530C Detector	
	DRX Core Detectors	
	PRO Detectors	
	DRX-L Detector	
	Focus Detectors	

Impacted by Vulnerability	Product	Patch Availability
Analog Systems / Not network connected		
Not impacted	QV-800 Digital Universal System	None
	Q-VISION	
	RAD-X Systems	
	Motion Mobile	
	ODYSSEY	
	QUEST	
	Tech Vision	
DryView – Windows XP Embedded Service Pack 3		
Not impacted as Print Spooler service is disabled by default	DRYVIEW 5700	None. Microsoft has not made a patch available for Windows XP systems.
	DRYVIEW 5950	
	DRYVIEW 6950	
DryView – Tux Linux		
Not impacted	DRYVIEW 5700	None
	DRYVIEW 5950	
	DRYVIEW 6950	
MyVue Center Kiosk Terminal – Windows 7		
Impacted	MyVue Center Kiosk Terminal	Upgrade to Windows 10
MyVue Center Kiosk Terminal – Windows 10		
Impacted	MyVue Center Kiosk Terminal	Patch qualification completed. See below for more information.
MyVue Center Kiosk Server – Windows Server 2008		
Impacted	MyVue Center Kiosk Server	Upgrade to Windows Server 2016
MyVue Center Kiosk Server – Windows Server 2012, 2016		
Impacted	MyVue Center Kiosk Server	Patch qualification completed. See below for more information.
INDUSTREX Non-Destructive Testing – Detectors		
Not applicable to device	HPX-DR 3543 PE Detector	None
	HPX-DR 4336 GH Detector	
	HPX-DR 2530 GH Detector	
	HPX-DR 2530 GC Detector	
	Exposure Interface Box (EIB)	
INDUSTREX Non-Destructive Testing – CR Systems		
Impacted	HPX-PRO Portable Digital System	

Impacted by Vulnerability	Product	Patch Availability
	HPX-1 Digital System	Customers may self-patch NDT systems. See below for more information.
	HPX-1 Plus Digital System	
INDUSTREX Non-Destructive Testing – Software		
Impacted	Digital Viewing Software	Customers may self-patch NDT systems. See below for more information.
	ayData NDT Archive	
INDUSTREX Non-Destructive Testing – Processors		
Not applicable to device	M43ic Processor	None
	M37 Plus Processor	

Vulnerability Details:
The Print Nightmare vulnerability is in the Windows Print Spooler service. Disabling this service will mitigate the vulnerability.

Vulnerability Mitigations:
The following information is provided for informational use only. The mitigations listed above for each system / version should be used as the preferred guidance from Carestream.

Mitigations from Microsoft CVE-2021-34527
Determine if the Print Spooler service is running

Run the following in Windows PowerShell:

```
Get-Service -Name Spooler
```

If the Print Spooler is running or if the service is not set to disabled, select one of the following options to either disable the Print Spooler service, or to Disable inbound remote printing through Group Policy:

Option 1 - Disable the Print Spooler service

If disabling the Print Spooler service is appropriate for your enterprise, use the following PowerShell commands:

```
Stop-Service -Name Spooler -Force
Set-Service -Name Spooler -StartupType Disabled
```

Impact of workaround

Disabling the Print Spooler service disables the ability to print both locally and remotely.

Option 2 - Disable inbound remote printing through Group Policy

You can also configure the settings via Group Policy as follows:

```
Computer Configuration / Administrative Templates /
Printers
Disable the “Allow Print Spooler to accept client
connections:” policy to block remote attacks.
```

You must restart the Print Spooler service for the group policy to take effect.

Impact of workaround

This policy will block the remote attack vector by preventing inbound remote printing operations. The system will no longer function as a print server, but local printing to a directly attached device will still be possible.

Option 3 – Apply the security updates

In addition to installing the Microsoft July 2021 security updates, you must confirm that the following registry settings are set to 0 (zero) or are not defined:

HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint
NoWarningNoElevationOnInstall = 0 (DWORD) or not defined (default setting)
UpdatePromptSettings = 0 (DWORD) or not defined (default setting)

Patch Availability:

Product	Version(s)	Patch Availability
ImageView systems	Any	Although not impacted due to the Print Spooler service being disabled, Carestream qualifies and releases all Microsoft patches every other month for ImageView systems. July 2021 patches will be qualified and made available in August 2021 in ImageView Security Update Pack (SUP) 2107. Contact your service provider for security updates or see: https://www.carestream.com/en/us/services-andsupport/cybersecurity-and-privacy for instructions on accessing the latest Security Update Packs on the Carestream service portal for self-installation.
DirectView systems	Any	DirectView Versions V5.7E and earlier may be impacted by Print Nightmare due to the Print Spooler service being enabled and not blocked by the firewall. DirectView Security Update Pack (SUP) 2010 is available and will disable the Print Spooler service, mitigating this vulnerability. This Security Update Pack is available for all DirectView systems (Windows XP & 7) and does not require Extended Security Updates. Carestream qualifies and releases all Microsoft patches every other month for DirectView systems. Although not required to mitigate this vulnerability, August 2021 patches will be qualified and made available in September 2021 in DirectView Security Update Pack (SUP) 2108. A Microsoft Extended Security Update (ESU) license is required to install these updates. Contact your service provider for more information. Contact your service provider for security updates or see: https://www.carestream.com/en/us/services-andsupport/cybersecurity-and-privacy for instructions on accessing the latest Security Update Packs on the Carestream service portal for self-installation.
Image Suite systems	Any	Patch qualification has been completed. See below for instructions on applying the Microsoft patches to Image Suite systems.

DRX-Excel (Duet)	Any	Carestream recommends that customers, as part of their risk management program, perform risk assessments to determine the risk of the Print Nightmare vulnerabilities on the medical device and to determine the appropriate response to that risk. For those seeking to remediate the vulnerability, Carestream has determined that of the three remediation options provided by Microsoft and documented above, Option #1 (disabling the Print Spooler service) carries the least risk of impacting the functionality of the medical device.
OMNI Products	Any	For Omni products, customers may apply patches directly from Microsoft using the provided links above.
MyVue Center	Any	Customers with Windows 7 systems should contact their service provider for information on upgrading the system to Windows 10. Verification of the July & August Microsoft security updates have been completed. Users may contact their service provider or install the July & August 2021 security updates by referencing the CVE links listed above.
Industrex NDT	Any	For NDT products and systems running NDT software, customers may apply patches directly from Microsoft using the provided links above.

This advisory will continue to be updated as patches are qualified and new information becomes available. For the latest advisory, see:

https://www.carestream.com/en/us/services-and-support

Please contact your Carestream sales representative to inquire about updating to the latest version of software.

Contact the Carestream Center of Excellence (COE) to coordinate patch installation or if you have additional questions. Service and support contacts can be found on Carestream's website at: https://www.carestream.com/en/us/services-and-support

Installing July 2021 Security Updates on Image Suite systems

- Before applying the security updates, you must first execute a Carestream script to configure the Microsoft Update services to the correct settings.
  Note: This step needs to be completed once. If this has already been done as part of a previous vulnerability remediation, then you may skip this step. There is no harm in performing this step a second time.
  To configure the Microsoft Update services:
  - Contact Carestream service and request Cyber Security End User Group Access to the Service Portal. For service contact information, see: https://www.carestream.com/en/us/services-and-support/world-wide-contacts
  - After receiving your credentials, you may logon to the Service Portal: https://my.carestream.com/
  - Navigate to Service Site → Health-Medical → Cybersecurity Customer Resource → Product Security Updates → Image Suite Security Updates → Image Suite Security Updates
  - Download InstallWsusSetupUtility.zip and extract the contents of the zip file.
  - In the newly extracted folder, go to InstallWsusSetupUtility and run InstallWsusSetup.bat as an Administrator.
  - Reboot the Image Suite system.
- Image Suite customers may now apply patches directly from Microsoft:
  - Customers running versions of Windows that are no longer supported should first contact service about upgrading to the latest version of Image Suite.
  - Download and install the latest Servicing Stack Update: https://msrc.microsoft.com/update-guide/vulnerability/ADV990001
    - On a Windows 8.1 system, this is KB5001403 https://support.microsoft.com/en-us/topic/kb5001403-servicing-stack-update-for-windows-8-1-windows-rt-8-1-and-windows-server-2012-r2-april-13-2021-718f317d-aa18-4b25-998d-d0a1abe6abfd
    - Supported Windows 10 systems should not require a servicing stack update.
  - Download and run the Adobe Flash removal package as Flash is no longer supported.
    - On Windows 10 systems, this is KB5004237.
    - https://support.microsoft.com/en-us/topic/july-13-2021-kb5004237-os-builds-19041-1110-19042-1110-and-19043-1110-ae798d3c-3de3-4c1f-b9d9-7391b71da889
    - On Windows 8.1 systems, customers may remove Adobe Flash manually through the Control Panel -> Add / Remove Programs
  - Download and install the correct July 2020 roll-up for your Windows 8.1 / Windows 10 system: https://msrc.microsoft.com/update-guide/releaseNote/2021-Jul
    - On a Windows 8.1 system, this is KB5004285 https://www.catalog.update.microsoft.com/Search.aspx?q=KB5004285
    - On a Windows 10 system, this is KB5004237 https://www.catalog.update.microsoft.com/Search.aspx?q=KB5004237

Note: .NET Framework and Edge Browser security updates have been qualified as part of previous product security advisories for Windows 10 systems only, and may also be installed:

- Download and install KB5000802 to patch the Edge Browser (if installed)
  https://support.microsoft.com/en-us/topic/march-9-2021-kb5000802-os-builds-19041-867-and-19042-867-63552d64-fe44-4132-8813-ef56d3626e14
  https://www.catalog.update.microsoft.com/Search.aspx?q=KB5000802
- Download and install the .NET Framework
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-24111

Carestream Product Security Guidance:

Carestream continuously evaluates the cybersecurity strategy of its products and often includes security patches and improvements with each software release. In order to maximize the resilience of your equipment, Carestream recommends customers keep their devices current by upgrading to the latest software release available for the product(s).

Carestream strongly recommends customers apply a layered security approach to protect all of their medical devices including Carestream equipment. Recommendations include but are not limited to:

- **Updates:** Apply software and security updates to the medical device when available.
- **Encryption:** Leverage Data at Rest and Data in Transit solutions to protect confidential data and the security of the system.
- **Physical Security:** Physically limit access to equipment when possible.
- **Role Based User Access**: Limit access to the equipment to authorized users only and minimize user privileges by role.
- **Network Isolation and Segmentation:** Firewalls, network segmentation, and/or virtual LANs should be used and configured to limit network communication of medical devices to only the addresses and ports required to support your workflow.
- **Endpoint & Network Monitoring:** Monitor the actions of devices at the endpoint and on the network through firewall, intrusion detection, endpoint audit logs by forwarding these logs to a Security Information and Event Management (SIEM) system.
- **Intended Use:** Only use Carestream products for intended use – do not check personal email, browse the internet, or install applications not required for the medical device

Updates to this advisory:

Future updates to this advisory will be posted to Carestream's website:
https://www.carestream.com/services-and-support/cybersecurity-and-privacy