Title:	**Bad Neighbor Vulnerability**
Advisory ID:	CARESTREAM-2020-05
Issue Date:	10-15-2020
Last Revision Date:	01-12-2021
CVE(s):	CVE-2020-16898, CVE-2020-16899

Advisory:
Carestream Health, Inc. is aware of the Bad Neighbor vulnerability that was published on 10-13-20 by Microsoft. This vulnerability affects devices running Windows 10 version 1709 through 2004, as well as Windows Server 2019 and Windows Server versions 1903, 1909, and 2004.

Are Carestream Products affected?
Yes, affected products are detailed below.

The following Carestream products are affected by this vulnerability:

- Image Suite Products
  - Perform the following steps to apply the Bad Neighbor patch and other security updates. This will bring the system up-to-date through October 2020.
    - Before applying the security updates, you must first execute a Carestream script to configure the Microsoft Update services to the correct settings. To do this:
      - 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://serviceportal.carestreamhealth.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*
      - Reboot the ImageSuite system.
    - Image Suite customers may now apply patches directly from Microsoft:
      - Download and install the correct Adobe patch for your Windows 10 system: https://msrc.microsoft.com/update-guide/en-US/vulnerability/ADV200010
      - Download and install the correct Windows 10 October 2020 roll-up for your Windows 10 system: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16898

- Omni Products
  - Omni Products customers can apply patches directly from Microsoft: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16898

For customers using versions of Windows 10 that are no longer supported by Microsoft, it is recommended that the system be updated to the latest version of Windows 10. If this is not possible, it is recommended to use the workaround suggested by Microsoft which is documented below.

The following Carestream products are not affected:

- Kiosk K2/K3/Puma
- Q-VISION / Q-VISION II
- Carestream products running ImageView software
- Carestream products running DirectView software
- DRX Detectors
- DryView Printers
- Duet (Excel)
- DRive
- QC
- POC
- QV-800 digital Universal System
- RAD-X
- Q-RAD (including ODYSSEY, QUEST, TechVision, Ascend digital)
- Tech Vision

Updates to this advisory:

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

Additional Information:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16898
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16899
- https://www.tenable.com/blog/microsoft-october-2020-patch-tuesday-87-cves-bad-neighbor-windows-tcp-ip-cve-2020-16898
- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/cve-2020-16898-bad-neighbor/

Workarounds:

Microsoft recommends this workaround to mitigate the risk of this vulnerability:

The following workaround may be helpful in your situation. In all cases, Microsoft strongly recommends that you install the updates for this vulnerability as soon as they become available even if you plan to leave this workaround in place:
Disable ICMPv6 RDNSS.
You can disable ICMPv6 RDNSS, to prevent attackers from exploiting the vulnerability, with the following PowerShell command. This workaround is only available for Windows 1709 and above**.**

```
netsh int ipv6 set int *INTERFACENUMBER* rabaseddnsconfig=disable
```

Note: No reboot is needed after making the change. See What's new in Windows Server 1709 for more information.

Carestream 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:

- **Physical Security**—Physically limit access to equipment when possible.
- **Role Based User Access**—Limit access to the equipment to authorized users only and minimizing 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.
- **Network Monitoring**—Monitor the actions of devices on the network through firewall, intrusion detection, and Security Information and Event Management (SIEM) logs.

January 2021