



Security Advisory

Revised Release Date: August 20th, 2019

CVE-2019-1181 | Remote Desktop Services Remote Code Execution Vulnerability

CVE-2019-1182 | Remote Desktop Services Remote Code Execution Vulnerability

AKA: DejaBlue

A remote code execution vulnerability exists in Remote Desktop Services – formerly known as Terminal Services – when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

To exploit this vulnerability, an attacker would need to send a specially crafted request to the target systems Remote Desktop Service via RDP.

The update addresses the vulnerability by correcting how Remote Desktop Services handles connection requests.

Reference:

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1181>

<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1182>

Overview:

Note: This Vulnerability is currently awaiting updated analysis and represents our best knowledge as of the most recent revision. As a result, the content is subject to change as further analysis is performed and the results are updated.

Canon Medical Systems Corporation continues to investigate the applicability of this vulnerability to Medical Imaging Devices manufactured by Canon Medical Systems Corporation.

CANON MEDICAL SYSTEMS USA, INC.

2441 Michelle Drive, Tustin CA 92780 | 800.421.1968

Canon Medical Systems USA, INC. 2018. All rights reserved. Design and specifications are subject to change without notice.

Made For life



Canon Medical Systems USA, Inc. has completed the investigation of the applicability of the vulnerability to InnerVision products.

Reference:

<https://www.malwaretech.com/2019/08/dejablue-analyzing-a-rdp-heap-overflow.html>

<https://www.aha.org/system/files/media/file/2019/08/dejablue-high-risk-windows-vulnerability-whitepaper.pdf>

Affected Canon Medical Systems Products:

XR/VL Medical Imaging Products	(Windows XP/Windows 7)
- Alphenix V8.x (Angio Workstation)	(Windows 7)
CT Medical Imaging Products	(Windows Server 2003 / Windows Server 2008)
- TSX series with SUREXtension option	(COT-49D)
MR Medical Imaging Products	(Windows 7)
- MRT series	(Windows 7)
InnerVision Service Processor	(Windows 7 / Windows 10)
InnerVision Service Processor Firewall	(Windows 7 / Windows 10)

Canon Medical Products that block Port 3389

(mitigated)

UL Medical Imaging Products	(Windows XP/Windows 7)
- Aplio 300, 400, 500	(Windows 7)
- Xario series	(Windows 7)
- Aplio i-Series 600, 700, 800, 900	(Windows 7)
- Aplio i-Series 600, 700, 800, 900	(Windows 10)
XR/VL Medical Imaging Products	(Windows7)
- Ultimax / Kalare (HDR-08A)	(Windows 7)

CANON MEDICAL SYSTEMS USA, INC.

2441 Michelle Drive, Tustin CA 92780 | 800.421.1968



Canon Medical Products that have RDP services disabled (mitigated)

XR/VL Medical Imaging Products (Windows7)

- | | |
|--------------------------------------|-------------|
| - Alphenix V8.x (DFP) | (Windows 7) |
| - Infinix-i V6.x (DFP) | (Windows 7) |
| - Infinix-i V6.x (Angio Workstation) | (Windows 7) |
| - Ultimix / Kalare (HDR-08A) | (Windows 7) |
| - Radrex(TFD-3000A) | (Windows 7) |

CT Medical Imaging Products (Windows 7)

- All TSX models

UL Medical Imaging Products (Windows 7)

- | | |
|-------------------------------------|--------------|
| - Aplio 300, 400, 500 | (Windows 7) |
| - Xario series | (Windows 7) |
| - Aplio i-Series 600, 700, 800, 900 | (Windows 7) |
| - Aplio i-Series 600, 700, 800, 900 | (Windows 10) |
| - UltraExtend FX | (Windows 7) |

Canon Medical Products that are not applicable

- | | |
|---------------------------------|-----------------------|
| - InnerVision TVR's | |
| - InnerVision eProtect | |
| - InnerVision Service Processor | (Windows XP) |
| - All Medical Imaging Products | (Windows XP or older) |

Canon Medical Products under investigation

- None

Resolution:

Medical Imaging Devices:

Canon Medical Systems Corporation will provide an update regarding implementation of the applicable Microsoft security patch.

CANON MEDICAL SYSTEMS USA, INC.

2441 Michelle Drive, Tustin CA 92780 | 800.421.1968



InnerVision Service Processor / InnerVision Service Processor Firewall:

If the VPN is functional as described in the White Paper, the applicable Microsoft OS updates will be rolled out automatically.

If assistance is needed, please contact Service Networking Support at ServiceNetworkingSupport@us.medical.canon or (855) 579-1968.

For Microsoft mitigations and workarounds please visit:

- <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1181>
- <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1182>

Notes:

Continue to check this advisory for updated information. Please email CybersecurityRiskManagement@us.medical.canon with any specific questions or issues.

Vulnerability Information

CVE-2019-1181

CVE-2019-1182

Additional notes:

For the Microsoft vulnerabilities listed below, although similar to the RDP vulnerability disclosed in this advisory, are not applicable to any products manufactured by Canon Medical Systems Corporation as they only apply to Win10 v1803 and above.

- **CVE-2019-1222:** <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1222>
- **CVE-2019-1223:** <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1223>
- **CVE-2019-1226:** <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1226>

Advisory Change Log

This is the first release of this Advisory

Initial Release Date: August 20th, 2019

CANON MEDICAL SYSTEMS USA, INC.

2441 Michelle Drive, Tustin CA 92780 | 800.421.1968