Security Advisory

Revised Release Date: January 15th, 2020

CVE-2020-0611 | Remote Desktop Services Remote Code Execution Vulnerability

A remote code execution vulnerability exists in the Windows Remote Desktop Client when a user connects to a malicious server. An attacker who successfully exploited this vulnerability could execute arbitrary code on the computer of the connecting client. 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 have control of a server and then convince a user to connect to it. An attacker would have no way of forcing a user to connect to the malicious server, they would need to trick the user into connecting via social engineering, DNS poisoning or using a Man in the Middle (MITM) technique. An attacker could also compromise a legitimate server, host malicious code on it, and wait for the user to connect.

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

REF:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0611

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. continues to investigate the applicability of the vulnerability to InnerVision products.

REFERENCE:

https://nvd.nist.gov/vuln/detail/CVE-2020-0611
https://www.us-cert.gov/ncas/alerts/aa20-014a

This vulnerability only affects the client side of the RDP connection for Windows 7 or Windows 10 devices. There is no applicability to WinXP or Win2000. No Canon Medical Systems Windows 7 or Windows 10 imaging equipment establishes a client side connection. Canon Medical Systems imaging equipment may offer RDP services as a server, however at no time will it function as a client.

CANON MEDICAL SYSTEMS USA, INC.
2441 Michelle Drive, Tustin CA 92780 | 800.421.1968

Canon Medical Systems USA, INC. 2020. All rights reserved. Design and specifications are subject to change without notice.

Made For life

Possible Affected Canon Medical Systems Products:

Affected Canon Medical Systems Products:

- No Canon Medical Systems imaging equipment
- InnerVision Service Processor (Windows 7 / Windows 10)
- InnerVision Service Processor Firewall (Windows 7 / Windows 10)

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.

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-2020-0611

Notes:

Continue to check this advisory for updated information.

Please email CybersecurityRiskManagement@us.medical.canon with any specific questions or issues.

Vulnerability Information : CVE-2020-0611

CANON MEDICAL SYSTEMS USA, INC.

2441 Michelle Drive, Tustin CA 92780 | 800.421.1968

Canon Medical Systems USA, INC. 2020. All rights reserved. Design and specifications are subject to change without notice.

Made For life

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 or Canon Medical Systems USA, Inc. as they only apply to Windows Servers.

- **CVE-2020-0609:** https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0609
- **CVE-2020-0610:** https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0609

Advisory Change Log

This is the first release of this Advisory

Initial Release Date: January 15th, 2020

CANON MEDICAL SYSTEMS USA, INC.

2441 Michelle Drive, Tustin CA 92780 | 800.421.1968

Canon Medical Systems USA, INC. 2020. All rights reserved. Design and specifications are subject to change without notice.

Made For life