Security Information: Remote desktop service vulnerability (CVE-2019-0708)

Canon Medical Systems Security Advisory

Overview

It was announced that there is a security vulnerability in the Remote Desktop Service (software for remote control from other computers) in the Windows OS. And there is a possibility that an attacker who successfully exploited this vulnerability could install software, view data, change data, or delete data. At this time, no attack code or attack damage that exploits this vulnerability has been confirmed.

Security Risk Evaluation Result

The evaluation results of Common Vulnerability Scoring System (CVSS) is 9.8 (critical level) and the degree of impact on confidentiality, integrity, and availability is also rated as "high". The attack method is as simple as sending a specially crafted RDP request to the remote desktop service of the target system.

Affected products

- VL Medical Imaging Products (Windows XP/Windows 7)
  - Infinix-i V4.x/V5.x (DFP) (Windows XP)
  - Infinix-i V4.x/V5.x (Angio Workstation) (Windows XP)
  - 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 XP/Windows 7)
  - MRT series (Windows XP)
  - MRT series (Windows 7)

Resolution

Canon Medical Systems Corporation will provide the Microsoft update for the following systems. Date is to be determined.

- CT TSX series with SUREXtension option (Windows Server 2003 / Windows Server 2008)
- MR MRT series (Windows 7)

Canon Medical Systems Corporation will provide risk mitigation measures for the following systems. Date is to be determined.

- VL Infinix-i V4.x/V5.x (DFP) (Windows XP)
- VL Infinix-i V4.x/V5.x (Angio Workstation) (Windows XP)
- VL Alphenix V8.x (Angio Workstation) (Windows 7)
- MR MRT series (Windows XP)

For inquiries concerning these subject products, please contact the nearest branch office, sales/service office.

Notes

It is known the followings as countermeasures for your network to reduce the possibility of security incident by this security vulnerability.

1) Control of communication protocol and communication port

The attack on the remote desktop service uses the following communication protocol and communication port. As one measure, it is valid to control not to allow those remote desktop service communication to our device. Alternatively, it is effective to change the communication port to something other than the default communication port.

Service Name	Protocol type and used port number
TermService	TCP 3389 port

END