

Customer Notice

April 13, 2020

RE: “BlueKeep” CVE-2019-0708 Vulnerabilities in the Hitachi ECHELON MR System

Dear Hitachi Healthcare Customer:

Windows recently identified a system vulnerability known as “BlueKeep”, or CVE-2019-0708, that has the potential to affect all Windows-based systems utilizing Remote Desktop Protocol (RDP) with Port 3389 exposed to the internet. Hitachi Healthcare has conducted an investigation into all of our products and has found the BlueKeep vulnerability only affects the ECHELON MRI running software versions v4.0B and v4.0C and a patch is required to remediate this vulnerability. No other Hitachi products require a patch to remediate this vulnerability as RDP is not actively utilized in any other Hitachi products and the issue only arises when RDP, that utilizes Port 3389, is exposed to the internet.

No other Hitachi MRI, Ultrasound or CT uses RDP or has any services running on Port 3389. As a result, no patch or update is required for these machines.

Hitachi Healthcare has installed a manufacturers “Compensating Control” in the form of a hardware firewall on all ECHELON systems, as the hardware firewall blocks this and other vulnerable ports. However, some customers have instructed us not to install the firewall and others customers have removed the firewall. Hitachi Healthcare strongly recommends that customers makes sure the hardware firewall is installed as Port 3389 is actively blocked by the hardware firewall if installed on your ECHELON System. Port 3389 is not actively blocked if the firewall is not installed on the ECHELON or you have removed the firewall after installation. If the hardware firewall is not installed, you should block Port 3389 on your network in some other fashion to improve the security of the ECHELON system. This will not affect the performance of the ECHELON.

Hitachi Healthcare will be patching the ECHELON software for all contract & warranty customers. No action is required on your part. Your service engineer will be contacting you to update the 4.0B or 4.0C software on your Echelon. Until the update, we recommend blocking RDP communication (3389/tcp and 3389/udp). Blocking the communication will not disrupt operations because RDP is not utilized.

If you have any questions on this matter, please contact Hitachi Regulatory Affairs at QualityRecords@hitachihealthcare.com.