Vulnerability Summary

An external security researcher has identified vulnerabilities in the Medtronic MyCareLink™ Patient Monitor (model numbers 24950 and 24952). This product is a remote monitoring system for patients with Medtronic implantable cardiac devices that allows patients to transmit device data to the Medtronic CareLink Network via a cellular connection for viewing by clinicians.

The vulnerabilities identified, when exploited together, allow privileged access to the operating system and visibility to product development code.

All vulnerabilities identified require physical access to both the home monitor and the patient at the same time and cannot be exploited via the internet. After assessing the impact of the vulnerabilities on patient safety, we have determined that the risks are controlled (meaning there is sufficiently low [acceptable] residual risk of patient harm). There are no known reports of patients being impacted or targeted by the identified vulnerabilities.

Medtronic is issuing automatic software updates to improve the overall security of affected monitors and is implementing additional mitigations to enhance remote monitoring security.

Medtronic encourages patients to only use home monitors obtained directly from Medtronic or their clinician. Patients should not use a pre-owned MyCareLink Patient Monitor or one that is purchased secondhand or online. Monitors obtained through unofficial means are at an increased risk for exploitation associated with the vulnerabilities identified.

Patients with questions or concerns about their MyCareLink Patient Monitors should contact Medtronic Patient Services at (800) 929-4043 or visit the Patient Services web site for more information.

At Medtronic, nothing is more important to us than the safety of our patients. We believe that the therapeutic benefits of our products far outweigh potential security risks, and we actively review our security practices to mitigate risks during premarket development and post-market use.

The full ICS-CERT security advisory can be found [here](#).