Vulnerability Summary

An external security research firm has identified vulnerabilities in Medtronic’s CareLink™ 2090 Programmer and its accompanying software deployment network.

Medtronic has assessed the vulnerabilities per our internal process. In an effort to continuously enhance system security, after receiving the vulnerability information from the research firm Medtronic added periodic integrity checks for certain files associated with the software deployment network.

After issuing this advisory on Feb. 27, 2018, Medtronic was made aware of additional vulnerabilities in the CareLink 2090 Programmer and its accompanying software deployment network. Medtronic has assessed the vulnerabilities and determined existing security controls in place mitigate this issue. The risks are controlled (meaning there is sufficiently low [acceptable] residual risk of patient harm).

Medtronic has not developed a product update to address these vulnerabilities but has identified compensating controls within this bulletin to help reduce the risk associated with these vulnerabilities.

Medtronic recommends that customers continue to follow the security guidance detailed in the Medtronic 2090 CareLink Programmer reference manual. This guidance includes maintaining good physical controls over the programmer and having a secure physical environment that prevents access to the 2090 programmer.

In addition, the 2090 programmer should be connected to a well-managed, secured computer network. If this is not possible, the 2090 programmer should be disconnected from the network (no impact to functionality), and updates may be received directly from a Medtronic representative.

Medtronic actively reviews its security practices to mitigate risks during premarket development and postmarket use.

The complete updated advisory issued by ICS-CERT can be found [here](#).