Vulnerability Summary

External security researchers Billy Rios and Jonathan Butts from WhiteScope LLC, identified vulnerabilities in Medtronic’s CareLink™ 2090 programmer and its accompanying Software Deployment Network (sometimes referred to as the Software Distribution Network or SDN). The SDN is a worldwide network hosted by Medtronic that allows the download of new or updated software to Medtronic’s CareLink 2090 and CareLink Encore™ 29901 programmers using a network connection.

Medtronic previously issued a security bulletin in February 2018, followed by an update in June 2018 specific to these vulnerabilities, which may allow an individual with malicious intent to update the programmers with non-Medtronic software.

New Findings
Further review of these vulnerabilities with the FDA, Billy Rios and Jonathan Butts revealed the potential for an attacker to remotely exploit some of these vulnerabilities. If not mitigated, these vulnerabilities could result in potential harm to a patient. **To date, we have not received a report of such an attack or patient harm.**

These vulnerabilities also exist with the CareLink Encore 29901 programmer and its association with the SDN. No other Medtronic programmers are impacted by this vulnerability.

Mitigations
To remediate these vulnerabilities and enhance cybersecurity of device programmers, Medtronic has disabled access to the SDN. When software updates are needed, a Medtronic representative will manually update, via a secured USB, all CareLink 2090 and CareLink Encore 29901 programmers. Medtronic is working on additional security updates for the impacted programmers and the SDN update process. We will implement these updates following regulatory agency approvals.

Customers should continue to use the programmers for programming, testing, and evaluating implanted devices. Network connectivity is not required for cardiovascular
Implantable electronic devices (CIED) programming and similar operation. Other Medtronic-provided features that require network connections are not impacted by these vulnerabilities (e.g. SessionSync™ and RemoteView™), and customers may continue to use such features.

Medtronic recommends that customers continue to follow the security guidance detailed in the CareLink 2090 programmer and CareLink Encore 29901 programmer reference manuals. This guidance includes maintaining good physical controls over the programmer and having a secure physical environment that prevents access to the CareLink 2090 or CareLink Encore 29901 programmer. Customers with questions or concerns about their programmers should contact Medtronic Technical Services at 800-638-1991.

Medtronic actively reviews its security practices to mitigate risks during pre-market development and post-market use.

The complete updated advisory issued by ICS-CERT can be found here.

Additional Resources:
FDA Communication
Medtronic Customer Communication