Vulnerability Summary

An external security researcher has identified potential vulnerabilities related to Medtronic’s N’Vision 8840 Physician Programmer and removable compact flash application card. The security researcher acquired one of Medtronic’s N’Vision 8840 Physician Programmers – a small, handheld device used solely by healthcare professionals to program certain Medtronic neuromodulation devices. The researcher’s report details that the compact flash application card used in the physician programmer may contain unencrypted patient personal health information if that information is not deleted following individual patient device programming. Additionally, it is possible that someone with physical access to the 8870 compact flash card and sufficient technical capability may be able to modify it to execute arbitrary code on the clinician programmer.

Medtronic has assessed this vulnerability per our internal process and found:

- Physical access to a physician programmer is needed to exploit the vulnerability.
- These devices are not commercially sold. These devices are intended for only healthcare practitioners. Any commercial sales to third parties are strictly prohibited.

Medtronic recommends that hospital and clinician users minimize risk by:

- Maintaining strict physical control of the application card
- Using only legitimately obtained application cards and not cards provided by any third party as firmware and system updates are provided directly by Medtronic using new application cards
- Properly disposing of all application cards after use, or returning cards to Medtronic so they can be securely discarded

Medtronic’s broader security structure is designed to limit a potential attacker’s ability to exploit system vulnerabilities. Some of these limitations include:

- The N’Vision 8840 programmer is not networked, and has no Wi-Fi capability, no USB connectivity and no Bluetooth connectivity capability. This eliminates the ability to access the device remotely or wirelessly.
- The N’Vision 8840 programmer is used and controlled by physicians in clinical environments. To insert malicious software onto a programmer, a potential attacker needs to have physical access to the programmer, place the malware on the 8870 program card, and then replace the programmer without detection – all within a clinical setting.
Any exploit that leverages this vulnerability requires physical access to the physician programmer and modification and/or replacement of the programming card without the physician being aware.

Additionally, these devices are not sold. They are loaned to physicians for use in programming Medtronic neuromodulation devices and subject to specific terms of service and use. While in a hospital’s possession, they remain the property of Medtronic and should be returned directly to Medtronic when they are no longer in use. Any sale or transfer of the 8840 and 8870 to any other party is strictly prohibited.

The application card stores PHI and PII as part of its normal operating procedure and should be handled, managed and secured in a manner consistent with the applicable laws for patient data privacy. Medtronic has not developed a product update to address the vulnerability but is reinforcing security practices within this bulletin to help reduce the risk associated with the vulnerability.

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

The full ICS-CERT security advisory can be found here.