SECURITY BULLETIN

Valleylab™ FT10 and Valleylab™ FX8 Electrosurgical Generator RSSH Vulnerabilities

11/07/2019

Medtronic

Vulnerability Summary

Medtronic actively reviews its security practices to mitigate risks during pre-market development and post-market use. Through this routine monitoring and testing, Medtronic identified security vulnerabilities in the software of the Valleylab™ FT10 and Valleylab™ FX8 electrosurgical generators. These products are used in operating rooms to assist surgeons and nurses during surgical procedures. These vulnerabilities could allow an unauthorized individual to take control of an electrosurgical generator, either through the network or through physical access to the device and change various settings.

To date, no cyberattack, data breach, or patient harm involving a Medtronic product has been observed or associated with this vulnerability.

Mitigation

Medtronic recommends that surgeons and nurses continue to use these devices as intended.

Customers should maintain good cyber hygiene practices by only connecting these devices to the hospital network when necessary and shutting them down between uses until the new software update is complete.

Medtronic has added security enhancements into a software update. These enhancements will mitigate the identified security vulnerabilities and protect the Valleylab™ device from malicious intrusion. **For the FT10 generators:** The update is available for certain versions. Customers should contact their Medtronic sales representative for more information. **For the FX8 generators:** Customers will be notified when the software update is available.

The update is recommended for enhanced security and an optimal user experience. Devices can continue to be used until the update is completed. Customers with multiple Valleylab™ generators will need to update each system individually.

Additional Resources

This software update addresses a separate cybersecurity vulnerability that affects the FT10 generator. [link to RFID bulletin]

All customers should contact their local sales representative for additional information. If you suspect cybersecurity-related activity has occurred with your device, please contact Medtronic at rs.assurancequality@medtronic.com.