SECURITY BULLETIN

Valleylab™ FT10 and Valleylab™ LS10 Electrosurgical Generator RFID Vulnerabilities

11/7/2019

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 our Valleylab™ FT10 and Valleylab™ LS10 electrosurgical generators. These products are used in operating rooms to assist surgeons and nurses during surgical procedures. These vulnerabilities could allow inauthentic surgical tools, which are devices that contain custom circuitry intended to clone or imitate new LigaSure™ devices, to be used with the electrosurgical generator, which could impact the performance of the LigaSure™ vessel-sealing system.

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 electrosurgical generators and the associated LigaSure™ devices as intended, and update to the latest software version. Because of the potential for inauthentic LigaSure™ devices to be recognized by the generators, customers should ensure that all LigaSure™ devices are purchased only from Medtronic or authorized Medtronic distributors.

Customers should maintain good cyber hygiene practices by only connecting the FT10 and LS10 electrosurgical generators to the hospital network when necessary and shutting them down between uses until the new software update is complete.

Medtronic released a software update for the Valleylab™ FT10 generator, which mitigates this security vulnerability. **For the FT10 generators:** The update is available for certain versions. Customers should contact their Medtronic sales representative for more information. **For the LS10 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 generator individually.

Additional Resources

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