GE

Security Bulletin

Overview

GE is aware of the recent reports of a widespread ransomware event, known as WannaCry, that is affecting numerous entities globally and we continue to monitor it closely. While the malware does not specifically target any GE products, any unpatched Windows-based system may be susceptible. GE takes this global threat very seriously and we strongly encourage all customers to follow industry best security practices.

Specifically, we recommend that our customers:1) not connect systems directly to the Internet, 2) regularly patch software as updates become available, and 3) continually monitor for new software updates.

Recommended mitigations

Information and support for GE Healthcare products is available through your GE Service contact, GE Service Call Center, or at http://www3.gehealthcare.com/en/support/security.

For all other GE products, GE recommends customers assess their systems and apply the Microsoft patches that were released on March 14, 2017 (MS17-010) and May 13, 2017 (KB4012598). Please see, https://blogs.technet.microsoft.com/mmpc/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/ and https://blogs.technet.microsoft.com/sudheesn/2017/05/17/patches-that-fix-the-vulnerability-for-ms17-010/.

Additionally, GE recommends the following mitigations be put in place. This includes, but is not limited to:

- Educating employees on security awareness.

- Placing GE products inside the control system network security perimeter, and having access controls, monitoring (i.e., Intrusion Detection System), and other mitigating technologies in place.

- Using strong network security practices, including network isolation and/or segregation where appropriate.

- If remote access is required, employing secure methods, such as Virtual Private Networks (VPNs) recognizing that the VPN is only as secure as the connected devices.

- Maintaining proper system backup capabilities and processes.

Product Support

For assistance or questions about the WannaCry malware as it relates to your GE product, please contact your local customer relationship manager, or for GE Healthcare products, refer to above. If you become aware of a vulnerability or other security concern involving a GE product, please notify GE at ge.security.com.