WannaCry Ransomware

Date: October 24, 2017

Overview:

Malware may encrypt or prevent access to documents, images, and other files until the victim pays the ransom (often in Bitcoin) for a key to unlock them. The nature of these cyber threats continues to rely on the vulnerabilities associated with the connectivity to external systems such as email servers and manual connection ports such as USB/flash drive devices and without user interaction, can spread into any vulnerable network device running Microsoft Windows. It spreads by exploiting a vulnerability of Server Message Block (SMB) in the Microsoft Windows operating system. The attack will pop-up messages letting you know you're the victim of ransomware and give you instructions for how to pay the ransom to get the decryption key.

Environment:

Networks containing Microsoft Windows based devices such as Supervisory Control and Data Aquisition (SCADA), Industrial Control Systems (ICS), Human Machine Interface (HMI), historian, legacy Alstom Depp data recorders, etc. may all be vulnerable.

- Microsoft Windows 10 devices are not vulnerable to WannaCry.
- For Microsoft supported operating systems/servers, Microsoft released a patch to protect against the WannaCry infection in March 2017.
- For some older, unsupported operating systems/servers, Microsoft released patches in May 2017.

Note: GE On-Site Monitors (OSMs) managed through the GE Monitoring & Diagnostics (M&D) center are patched regularly. The WannaCry patch was pushed to the OSM fleet in April 2017 so they are all protected. The M&D patch management program ensures that security patches for M&D systems are tracked, evaluated, tested, and installed within policy directives when a security patch is applicable. Exceptions are tracked closely and additional mitigations are applied where remediation cannot be ensured. The architecture and practices of M&D services attempts to minimize exposures by applying numerous, overlapping safeguards to reduce the impact of attacks. While system patching is a suitable defense, it is just one of many controls used and is not relied on as the only defense. In addition, GE Power restricts the use of SMB communications to customer connected environments, which significantly reduces the spread of this threat. Legacy Alstom Depp data recorders are not managed or maintained by GE. As a result, these may be vulnerable to WannaCry ransomware.

Resolution:

To address WannaCry vulnerabilities, install the applicable software patch by following steps 1 to 3 below.

1. Take an image backup of the Microsoft Windows based device to be updated (HMI,Historian, etc.)

2. Update the antivirus definitions/software.

3. Run and install the application Microsoft Windows patch. In rare instances, Microsoft or other updates/patches may impact the device's function. As such, new updates should be tested on one or two devices before being propagated to the entire plant.

Note: Users enrolled in the Cyber Asset Protection (CAP) program offered by GE Digital Solutions should have already received the patch in the GE Control Solutions M3 2017 CAP deliverables. If not installed, deploy this patch and successive patches as early as possible to mitigate this vulnerability. Users with HMIs running operating systems below Windows XP can contact GE Digital Solutions (controlsmodificationquote@ge.com) for HMI/historian upgrade options since these operating systems are no longer supported by Microsoft.

Attachments

- Windows 7 for 32-bit (KB4012212).zip
- Windows 7 for 64-bit (KB4012212).zip
- Windows Server 2003 for 32-bit (KB4012598).zip
- Windows Server 2003 for 64-bit(KB4012598).zip
- Windows Server 2008 for 32-bit (KB4012598).zip
- Windows Server 2008 for 64-bit(KB4012598).zip
- Windows Server 2008 R2 for 64-bit(KB4012212).zip
- Windows XP SP2 for 64-bit(KB4012598).zip
- Windows XP SP3 (KB4012598).zip

https://gepowerpac.service-now.com/kb_view.do?sysparm_article=KB0023936

GE Power Product Security Incident Response Team (PSIRT)

GE is committed to helping ensure the security of its customer base. To report product security issues and to request security support, contact GE Power PSIRT at www.ge.com/power/cybersecurity or GEPowerCVD@ge.com.