# WannaCry Response

*METASYS*® BUILDING AUTOMATION SYSTEM (BAS) AND WANNACRY | JUNE 2017

## *METASYS* BAS AND THE WANNACRY RANSOMWARE THREAT

On Friday, May 12, 2017, a previously unknown strain of ransomware began affecting computer systems across the globe. Known as WannaCry or Wcry, the ransomware has caused significant disruptions at various types of organizations – banks, hospitals, telecommunications providers and other mission-critical organizations.

Ransomware is an evolving type of malware (i.e. malicious code) that blocks access to sensitive files and/or electronic devices by automatically encrypting them upon infection.

WannaCry affects computers running some older and unpatched versions of the Microsoft® Windows® operating systems. Initial reports indicate that this ransomware may first be introduced to a network by users clicking on a malicious link or opening an infected email attachment. Once introduced, the malware then spreads to other computers using a Windows Server Message Block (SMB) vulnerability. Files on affected computers are then encrypted for a ransom.

### Potential Impact to *Metasys* Systems

Any computer running older or unpatched versions of the Windows operating system is potentially vulnerable to WannaCry. As a result, *Metasys* software, tools, and applications may be vulnerable if they have been installed on computers running older or unpatched versions of the Windows operating system. Listed below are some examples of *Metasys* software, tools, and applications that are typically installed on Windows-based computers, and therefore, could be vulnerable to WannaCry:

- Extended and Application & Data Server (ADX, ADS)
- Open Data Server (ODS)
- Ready Access Portal (RAP) Server
- System Configuration Tool (SCT)
- Controller Configuration Tool (CCT)
- NAE85 Network Automation Engine software
- NIE89 Network Integration Engine software
- LonWorks Control Server (LCS85) software

*Metasys* Network Automation and Integration Engines that are part of the *Metasys* NxE55 platform may also be vulnerable to WannaCry.

- *Metasys* network engines at newer releases, especially *Metasys* Release 8.1 (the latest *Metasys* release), are less vulnerable, as their internal firewalls are enabled by default, thus blocking Port 445
- *Metasys* engines at Releases 5.2-7.0 may be potentially more vulnerable

NOTE: the *Metasys* NxE25/35/45 network engines are not affected by the WannaCry ransomware because they are built on the Windows CE operating system.

For a detailed list of potentially vulnerable *Metasys* servers and engines, contact your Johnson Controls representative.

**Immediate Actions Required for *Metasys* Customers**

- Apply the Microsoft Security Patch MS17-010 to servers and client computers that run, or interface to, *Metasys* software
- Contact your Johnson Controls representative if any *Metasys*-specific patches are required for your NxE55 platform
- Follow best practices of backing up the entire *Metasys* archive database with the System Configuration Tool, and use the *Metasys* Database Manager to back up important trend, event, and audit information
- Turn on the firewall for *Metasys* NxE55 Series network engines at Release 5.2, 6.x, and 7.0, which block port 445 by default*

*Customers whose engines are listed for Smoke Control should check with their Johnson Controls representatives before taking any action. We are currently working with UL to determine the best approach for protecting life-safety systems.

**Additional Recommendations for Securing *Metasys* Systems**

As a general best practice, *Metasys* customers should stay current with their Metasys systems, as doing so is one the most effective ways to help prevent against cyberattacks.

- Upgrade to *Metasys* 8.1 as it helps block the WannaCry virus with an automatically enabled operational internal host firewall to block SMB network protocol port 445
- Use this as an opportunity to work with your Johnson Controls representative to ensure IT security best practices are being applied across your building network

**Additional Resources:**

- Johnson Controls WannaCry Response FAQs
- Network and IT Guidance Technical Bulletin (LIT-12011279)
- *Metasys* System Configuration Guide (LIT-12011832)

For more information on how WannaCry potentially impacts your *Metasys* system or for help implementing the required actions, contact your Johnson Controls representative at your earliest convenience.
Or contact the Johnson Controls Product Security Incident Response Team at beproductsecurity@jci.com.