CHRISTIE

Technical Bulletin

Touch panel controller security for Christie cinema projectors

This bulletin provides security information about the touch panel controller (TPC) software image.

Christie is aware of recent software exploits such as WannaCry and similar cryptoworms. Such cryptoworms spread by exploiting the Windows Server Message Block (SMB) and simple file sharing protocol.

No TPC software updates are required to address the WannaCry exploit based on the following:

- SMB/simple file sharing is disabled on the TPC software image for all Christie cinema projectors; therefore, the TPC is not vulnerable to exploits that rely on this protocol.
- Christie Series 1 cinema projectors run the Windows CE operating system and the WannaCry cryptoworm cannot run on Windows CE for ARM devices.
- Christie Series 3 cinema projectors do not run a Windows-based operating system and the WannaCry cryptoworm only exploits Windows-based system.
- CP42LH systems use a Laser Bank Manager that communicates with the rack and TPC on a private network. The Laser Bank Manager is never connected to the theatre network and will not be exposed to the WannaCry cryptoworm.

Affected products

This bulletin applies to the following Cinema projectors.

- All Christie Series 1 cinema projectors
- All Christie Series 2 cinema projectors
- All Christie Series 3 cinema projectors
- CP42LH (3P and 6P) systems

Technical support

Technical support for Christie products is available at:

- North and South America: +1-800-221-8025 or Support.Americas@christiedigital.com
- Europe, Middle East, and Africa: +44 (0) 1189 778111 or Support.EMEA@christiedigital.com
- Asia Pacific: +65 6877-8737 or Support.APAC@christiedigital.com
- Christie Managed Services: +1-800-550-3061 or NOC@christiedigital.com