

FOR IMMEDIATE RELEASE
May 6, 2019

Contact: Tracy Cullen
ph. 1-703-8413282

DICOM STATEMENT ON REPORTED MALWARE VULNERABILITY

DICOM SECURITY GROUP PROVIDES USER STRATEGIES TO MITIGATE RISK

Arlington, VA, May 6, 2019 – *DICOM, the international Standard to transmit, store, retrieve, print, process, and display medical imaging information, issued the following statement regarding a potential vulnerability in the preamble defined by the DICOM File format which could allow DICOM files to be stored on media with executable malware inserted.*

“DICOM files on media, like CDs and DVDs, include a 128-byte preamble at the start of the file. The intended purpose of the preamble is to allow both DICOM software and non-DICOM software to process the same file. This is a useful feature for both backward and forward compatibility of some types of medical imaging devices.

“However, as reported, the potential exists to abuse the 128-byte preamble allowing DICOM files to be stored on media with executable malware inserted. A malicious actor could modify a DICOM file so that it is treated as both an executable program and as a DICOM file, and then a user might be convinced to execute the file via social engineering. Alternatively, a separate malicious actor that knew about the embedded executable and had access to the modified file could install and execute the malware. This type of intrusion is referred to as a multi-phase attack.

“The risks of such an exploit can be mitigated. Just as recipients of strange email attachments should be cautious about opening them, programs that process DICOM media files should take precautions. Virus scanning software should scan DICOM media files and not assume DICOM media files are safe. Data import systems should have file execution disabled when reading CD/DVDs.

“To provide more detailed information about this matter and potential risk and mitigation strategies, DICOM has published a Frequently Asked Questions (FAQ) available at <https://www.dicomstandard.org/dicom-in-the-news/>

“The DICOM security workgroup welcomes efforts to strengthen systems against cybersecurity attacks, to raise awareness of potential attack vectors, and to help users and developers understand how to guard against them.”

DICOM® (Digital Imaging and Communications in Medicine) is the international Standard to transmit, store, retrieve, print, process, and display medical imaging information. DICOM® makes medical imaging information interoperable, integrates image-acquisition devices, PACS, workstations, VNAs and printers from different manufacturers, is actively developed and maintained to meet the evolving technologies and needs of medical imaging, and is free to download and use. The goal of the DICOM Standard is to achieve compatibility and improve workflow efficiency between imaging systems and other information systems in healthcare environments worldwide. DICOM® is the registered trademark of the National Electrical Manufacturers Association (NEMA) for its Standards publications relating to digital communications of medical information.”

The National Electrical Manufacturers Association (NEMA) represents nearly 325 electrical equipment and medical imaging manufacturers that make safe, reliable, and efficient products and systems. Our combined industries account for 360,000 American jobs in more than 7,000 facilities covering every state. These industries produce \$106 billion in shipments and \$36 billion in exports of electrical equipment and medical imaging technologies per year.