

3M RFID and Virus Protection

You may have heard or read about possible vulnerabilities in RFID software that allow RFID tags to be infected with viruses that may, in turn, infect the database used by the software and spread to other RFID tags. The information provided below addresses how 3M continually takes proactive measures to help ensure the quality and security levels of 3M™ RFID Systems and components.

While there is current concern around RFID tags and the threat of viruses, the fact is that any data entry means can cause the type of problem described by the research on RFID viruses. The information stored on the RFID tag is just data, not a malicious “program”. The RFID virus attacks that made headlines in the news were simulated by taking advantage of poorly designed software by inputting more data than was expected or by formatting data in unexpected ways. This caused unexpected and poor software behavior. This type of problem is not specific to RFID tags. It can also be caused by other data input means such as scanning a barcode or manually typing.

All well-designed software should read only the data that is needed, and validate and interpret it appropriately for the system. 3M™ RFID Tags and software are designed to work together to avoid vulnerabilities such as those described above. For example, each RFID tag’s data has a rigidly defined format that is validated for content and expected values, making it difficult for malicious exploitation. In addition, 3M periodically reviews the software programming code to identify and update areas to reduce the chance for a potential issue. These proactive measures are taken by 3M to help ensure the quality and security levels expected by our customers

5/17/06