Según un informe de la industria, las máquinas de imágenes médicas que ejecutan software obsoleto como Windows 2000, pueden brindar a los piratas informáticos el control de la información confidencial de pacientes que puede costar a los hospitales millones de dólares.

Los hackers que ingresan a los hospitales y sus redes pueden conectarse fácilmente a los dispositivos de imágenes de ultrasonido que ejecutan software antiguo que comúnmente se utiliza para controlar embarazos y otras afecciones, según informó el jueves el especialista en seguridad cibernética, Check Point Software Technologies.

Ataques como el ataque del ransomware WannaCry de 2017 que afectó a las computadoras de por lo menos 100 países, incitaron a Check Point a investigar las posibles técnicas de los piratas informáticos.

El virus se propagó principalmente por medio de programas que carecían de actualizaciones de seguridad recientes y que solo le costaron al Servicio Nacional de Salud del Reino Unido, 104 millones de dólares en costos de producción y tecnología de la información perdidos, según un informe del año pasado del Departamento de Salud y Asistencia Social.

«Queríamos mostrar cómo esto podría suceder», dijo Gil Messing, portavoz de Check Point, enfatizando que el problema no era con los dispositivos o los fabricantes, sino con el software obsoleto.

La vulnerabilidad puede provenir de dispositivos de salud que se ejecutan en un software tan antiguo que no existen parches ni actualizaciones, según el informe. Los hospitales por lo general no quieren desconectar las máquinas costosas para actualizaciones que llevan tiempo, ya que pierden pacientes y cuesta dinero.

Las soluciones incluyen un mejor cifrado de los archivos, mediante el uso de soluciones de seguridad más avanzadas e integrales y la separación de los datos de los pacientes de las redes de TI, afirmó Check Point en su blog.