La implementación inadecuada de los estándares de telecomunicaciones, las amenazas de la cadena de suministro y las debilidades en la arquitectura de los sistemas podrían plantear importantes riesgos de ciberseguridad para las redes 5G, lo que podría convertirlas en un objetivo lucrativo para que los hackers y adversarios de los estados nacionales los exploten en busca de inteligencia valiosa.

El análisis, que tiene como objetivo identificar y evaluar los riesgos y vulnerabilidades introducidos por la adopción de 5G, fue publicado el lunes por la Agencia de Seguridad Nacional de Estados Unidos (NSA), en asociación con la Oficina del Director de Inteligencia Nacional (ODNI), el Departamento de Seguridad Nacional (DHS) y la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA).

> *«A medida que las nuevas políticas y normas 5G son liberados, sigue existiendo la posibilidad de que las amenazas afecten al usuario final. Por ejemplo, los estados nacionales pueden intentar ejercer una influencia indebida sobre los estándares que benefician sus tecnologías patentadas y limitan las opciones de los clientes para usar otros equipos o software»,* dice el informe.

Específicamente, el informe cita la influencia indebida de naciones adversarias en el desarrollo de estándares técnicos, que pueden allanar el camino para la adopción de tecnologías y equipos patentados que no son de confianza y que podrían ser difíciles de actualizar, reparar y reemplazar.

También son motivo de preocupación, según el informe, los controles de seguridad opcionales incorporados en los protocolos de telecomunicaciones, que, si no los implementan los operadores de red, podrían dejar la puerta abierta a ataques maliciosos.

Una segunda área de preocupación destacada por la NSA, ODNI y CISA, es la cadena de suministro. Los componentes adquiridos de proveedores externos y proveedores de servicios podrían ser falsificados o comprometidos, con fallas de seguridad y malware inyectado durante el proceso de desarrollo inicial, lo que permite a los actores de amenazas explotar

las vulnerabilidades en una etapa posterior.

> *«Los componentes falsificados comprometidos podrían permitir a un actor malintencionado afectar la confidencialidad, integridad o disponibilidad de los datos que viajan a través de los dispositivos y moverse lateralmente a otras partes más sensibles de la red»,* dice el análisis.

Esto también podría tomar la forma de un ataque a la cadena de suministro de software en el que se agrega código malicioso a un módulo que se entrega a los usuarios objetivo, ya sea infectando el repositorio de código fuente o secuestrando el canal de distribución, lo que permite a los clientes desprevenidos implementar los componentes en sus redes.

Finalmente, las debilidades en la propia arquitectura 5G podrían usarse como punto de partida para ejecutar una variedad de ataques. La principal de ellas es la necesidad de respaldar la infraestructura de comunicaciones heredada 4G, que viene con su propio conjunto de deficiencias inherentes que pueden ser explotadas por actores malintencionados.

Otro problema es la gestión inadecuada de segmentos que podría permitir a los adversarios obtener datos de distintos segmentos e incluso interrumpir el acceso a los suscriptores.

Un estudio publicado por AdaptiveMobile en marzo de 2021, encontró que las fallas de seguridad en el modelo de corte que podrían reutilizarse para permitir el acceso a datos y llevar a cabo ataques de denegación de servicio entre diferentes cortes de red en la red 5G de un operador móvil.

> *«Para alcanzar su potencial, los sistemas 5G requieren un complemento de frecuencias de espectro (bajo, medio y alto) porque cada tipo de frecuencia ofrece beneficios y desafíos únicos. Con un número cada vez mayor de dispositivos que compiten por el acceso al mismo espectro, el uso compartido del espectro es cada*

> *vez más común. El uso compartido del espectro puede brindar oportunidades para que los malos actores interfieran con rutas de comunicación no críticas, afectando de forma negativa las redes de comunicación más críticas»,* dice el informe.

Al identificar las políticas y los estándares, la cadena de suministro y la arquitectura de los sistemas 5G como los tres principales vectores de amenazas potenciales, la idea es evaluar los riesgos que plantea la transición a la nueva tecnología inalámbrica, así como garantizar el despliegue de una infraestructura 5G segura y confiable.

> *«Estas amenazas y vulnerabilidades podrían ser utilizadas por actores de amenazas malintencionados para impactar de forma negativa a organizaciones y usuarios. Sin un enfoque continuo en los vectores de amenazas 5G y una identificación temprana de las vulnerabilidades en la arquitectura del sistema, las nuevas vulnerabilidades aumentarán el impacto de los incidentes cibernéticos»,* dijeron las agencias.