Investigadores de ciberseguridad han revelado múltiples fallos de seguridad en los módems celulares Cinterion que podrían ser potencialmente explotados por actores maliciosos para acceder a información sensible y lograr la ejecución de código.

> *«Estas vulnerabilidades incluyen fallos críticos que permiten la ejecución remota de código y la escalada no autorizada de privilegios, lo que representa riesgos sustanciales para las redes de comunicación integral y los dispositivos IoT fundamentales para los sectores industrial, de salud, automotor, financiero y de telecomunicaciones»*, dijo Kaspersky.

Los módems Cinterion fueron desarrollados originalmente por Gemalto antes de que el negocio fuera adquirido por Telit de Thales como parte de un acuerdo anunciado en julio de 2022.

Los hallazgos se presentaron en el OffensiveCon celebrado en Berlín el 11 de mayo. La lista de ocho fallas es la siguiente:

- CVE-2023-47610 (puntuación CVSS: 8.1) – Una vulnerabilidad de desbordamiento de búfer que podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema objetivo enviando un mensaje SMS especialmente diseñado.
- CVE-2023-47611 (puntuación CVSS: 7.8) – Una vulnerabilidad de gestión de privilegios incorrecta que podría permitir a un atacante local con privilegios bajos elevar los privilegios al nivel del fabricante en el sistema objetivo.
- CVE-2023-47612 (puntuación CVSS: 6.8) – Una vulnerabilidad de archivos o directorios accesibles a partes externas que podría permitir a un atacante con acceso físico al sistema objetivo obtener acceso de lectura/escritura a cualquier archivo y directorio en el sistema objetivo, incluidos archivos y directorios ocultos.
- CVE-2023-47613 (puntuación CVSS: 4.4) – Una vulnerabilidad de traversal de ruta relativa que podría permitir a un atacante local con privilegios bajos escapar de directorios virtuales y obtener acceso de lectura/escritura a archivos protegidos en el sistema objetivo.

- CVE-2023-47614 (puntuación CVSS: 3.3) – Una vulnerabilidad de exposición de información sensible que podría permitir a un atacante local con privilegios bajos revelar rutas virtuales ocultas y nombres de archivos en el sistema objetivo.
- CVE-2023-47615 (puntuación CVSS: 3.3) – Una vulnerabilidad de exposición de información sensible a través de variables de entorno que podría permitir a un atacante local con privilegios bajos obtener acceso no autorizado al sistema objetivo.
- CVE-2023-47616 (puntuación CVSS: 2.4) – Una vulnerabilidad de exposición de información sensible que podría permitir a un atacante con acceso físico al sistema objetivo acceder a datos sensibles en el sistema objetivo.

La más grave de las debilidades es CVE-2023-47610, una vulnerabilidad de desbordamiento de montón en el módem que permite a los atacantes remotos ejecutar código arbitrario a través de mensajes SMS.

Además, el acceso podría ser utilizado para manipular la memoria RAM y flash, lo que permite a los atacantes ejercer más control sobre el módem sin autenticación o requerir acceso físico.

Las vulnerabilidades restantes provienen de fallos de seguridad en el manejo de MIDlets, que se refieren a aplicaciones basadas en Java que se ejecutan dentro de los módems. Podrían ser abusados para eludir comprobaciones de firma digital y permitir la ejecución de código no autorizado con privilegios elevados.

Los investigadores de seguridad Sergey Anufrienko y Alexander Kozlov han sido acreditados con el descubrimiento e informe de las fallas, que fueron reveladas formalmente por Kaspersky ICS CERT en una serie de avisos publicados el 8 de noviembre de 2023.

> *«Dado que los módems suelen estar integrados de forma similar a una muñeca rusa dentro de otras soluciones, con productos de un proveedor apilados sobre los de otro, compilar una lista de productos finales afectados es un desafío»,* dijo Evgeny Goncharov, jefe de Kaspersky ICS CERT.

Para mitigar posibles amenazas, se recomienda a las organizaciones desactivar las capacidades de mensajería SMS no esenciales, emplear Nombres de Punto de Acceso (APN) privados, controlar el acceso físico a los dispositivos y realizar auditorías y actualizaciones de seguridad regulares.