La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) publicó tres avisos de Sistemas de Control Industrial (ICS) sobre múltiples vulnerabilidades en el software de ETIC Telecom, Nokia y Delta Industrial Automation.

Entre ellos destaca un conjunto de tres vulnerabilidades que afectan al servidor de acceso remoto (RAS) de ETIC Telecom, que *«podría permitir que un atacante obtenga información confidencial y comprometa el dispositivo vulnerable y otras máquinas conectadas»,* dijo CISA.

Esto incluye CVE-2022-3703 (puntaje CVSS: 9.0), una vulnerabilidad crítica que se deriva de la incapacidad del portal web RAS para verificar la autenticidad del firmware, lo que hace posible deslizar un paquete falso que otorga acceso de puerta trasera al adversario.

Otras dos vulnerabilidades se relacionan con un error de recorrido de directorio en la API de RAS (CVE-2022-41607, puntaje CVSS: 8.6) y un problema de carga de archivo (CVE-2022-40981, puntaje CVSS: 8.3) que se puede explotar para leer archivos arbitrarios y cargar archivos maliciosos que pueden comprometer el dispositivo.

A la empresa israelí de ciberseguridad industrial OTORIO, se le atribuye el descubrimiento y la notificación de las fallas. Todas las versiones de ETIC Telecom RAS 4.5.0 y anteriores son vulnerables, con los problemas abordados por la empresa francesa en la versión 4.7.3.

El segundo aviso de CISA se refiere a tres vulnerabilidades en el módulo de sistema común ASIK AirScale 5G de Nokia (CVE-2022-2482, CVE-2022-2483 y CVE-2022-2484), que podrían allanar el camino para la ejecución de código arbitrario y la funcionalidad de detención de seguridad de arranque. Todas las vulnerabilidades tienen una calificación de 8.4 en la escala de gravedad CVSS.

> *«La explotación exitosa de estas vulnerabilidades podría resultar en la ejecución de un núcleo malicioso, la ejecución de programas maliciosos arbitrarios o la ejecución de programas Nokia modificados»*, dijo CISA.

Se dice que la compañía finlandesa de telecomunicaciones publicó instrucciones de mitigación para las fallas que afectan a las versiones 474021A.101 y ASIK 474021A.102 de ASIK. La agencia recomienda que los usuarios se comuniquen directamente con Nokia para obtener más información.

Finalmente, la autoridad de seguridad cibernética también advirtió sobre una vulnerabilidad de cruce de ruta (CVE-2022-2969, puntaje CVSS: 8.1) que afecta a los productos DIALink de Delta Industrial Automation, y podría aprovecharse para plantar código malicioso en dispositivos específicos.

La vulnerabilidad se solucionó en la versión 1.5.0.0 Beta 4, que CISA dijo que se puede obtener comunicándose con Delta Industrial Automation directamente, o a través de la ingeniería de aplicaciones de campo (FAE) de Delta.