Investigadores de seguridad cibernética revelaron detalles sobre 15 vulnerabilidades de seguridad en el sistema de administración de red (NMS) Siemens SINEC, algunas de las cuales podrían ser encadenadas por un atacante para lograr la ejecución remota de código en los sistemas afectados.

> *«Las vulnerabilidades, de ser explotadas, presentan una serie de riesgos para los dispositivos de Siemens en la red, incluidos ataques de denegación de servicio, fugas de credenciales y ejecución remota de código en ciertas circunstancias»*, dijo la compañía de seguridad industrial Claroty.

Las fallas en cuestión, rastreadas desde CVE-2021-33722 hasta CVE-2021-33736, fueron abordadas por Siemens en la versión V1.0 SP2 Update 1, como parte de las actualizaciones enviadas el 12 de octubre de 2021.

> *«El más grave podría permitir que un atacante remoto autenticado ejecute código arbitrario en el sistema, con privilegios del sistema, bajo ciertas condiciones»*, dijo Siemens.

La principal de las vulnerabilidades es CVE-2021-33723 (puntuación CVSS: 8.8), que permite escalar privilegios a una cuenta de administrador y podría combinarse con CVE-2021-33722 (puntuación CVSS: 7.2), una falla transversal de ruta, para ejecutar código arbitrario de forma remota.

Otra vulnerabilidad muy notables se relaciona con un caso de inyección SQL (CVE-2021-33729, puntaje CVSS: 8.8) que podría ser explotada por un hacker autenticado para ejecutar comandos arbitrarios en la base de datos local.

> *«SINEC se encuentra en una posición central poderosa dentro de la topología de la*

> *red porque requiere acceso a las credenciales, claves criptográficas y otros secretos que le otorgan acceso de administrador para administrar dispositivos en la red»,* dijo Noam Moshe, de Claroty.

> *«Desde la perspectiva de un atacante que lleva a cabo un tipo de ataque de vivir de la tierra donde se abusa de las credenciales legítimas y las herramientas de red para realizar actividades maliciosas, acceso y control, SINEC coloca a un atacante en una posición privilegiada para: reconocimiento, movimiento lateral y escalada de privilegios».*