Investigadores de seguridad cibernética descubrieron vulnerabilidades críticas en las implementaciones de VPN industriales utilizadas principalmente para proporcionar acceso remoto a redes de tecnología operativa (OT), que podrían permitir a los hackers sobrescribir datos, ejecutar código malicioso y comprometer los sistemas de control industrial (ICS).

Un nuevo informe publicado por la compañía de seguridad cibernética industrial, Claroty, demuestra múltiples vulnerabilidades graves en instalaciones VPN de nivel empresarial, incluido el servidor Secomea GateManager M2M, Moxa EDR-G902 y EDR-G903, y el cliente eCatcher VPN de HMS Networks eWon.

Estos productos vulnerables se utilizan ampliamente en industrias basadas en el campo, como el petróleo y gas, los servicios públicos de agua y los servicios eléctricos para acceder, mantener y monitorear remotamente ICS y dispositivos de campo, incluidos controladores lógicos programables (PLC) y dispositivos de entrada/salida.

Según los investigadores de Claroty, la explotación exitosa de las vulnerabilidades puede brindar a un atacante no autenticado acceso directo a los dispositivos ICS y potencialmente causar daño físico.

En GateManager de Secomea, los investigadores descubrieron múltiples fallas de seguridad, incluida una vulnerabilidad crítica (CVE-2020-14500) que permite sobrescribir datos arbitrarios, ejecutar código arbitrario o causar una condición DoS, ejecutar comandos como root y obtener contraseñas de usuario debido al uso de un tipo de hash débil.

GateManager es un servidor de acceso remoto ICS ampliamente utilizado implementado en todo el mundo como una solución SaaS basada en la nube, que permite a los usuarios conectarse a la red interna desde Internet por medio de un túnel encriptado mientras evita las configuraciones del servidor.

La falla crítica, identificada como CVE-2020-14500, afecta al componente GateManager, la instancia de enrutamiento principal en la solución de acceso remoto Secomea. La falla se produce debido a un manejo inadecuado de algunos de los encabezados de solicitud HTTP

proporcionados por el cliente.

Esta falla puede explotarse remotamente y sin requerir ninguna autenticación para lograr la ejecución remota de código, lo que podría resultar en obtener acceso completo a la red interna de un cliente, junto con la capacidad de descifrar todo el tráfico que pasa a través de la VPN.

En los servidores VPN industriales Moxa EDR-G902 y EDR-G903, los investigadores descubrieron un error de desbordamiento de búfer basado en pila (CVE-2020-14511), en el servidor web del sistema que puede activarse simplemente al enviar una solicitud HTTP especialmente diseñada, que eventualmente permite a los atacantes llevar a cabo ejecución remota de código sin necesidad de credenciales.

Los investigadores de Claroty también probaron eCatcher de HMS Networks, un cliente VPN patentado que se conecta al dispositivo eWon VPN de la compañía, y descubrieron que el producto es vulnerable a un desbordamiento de búfer crítico basado en pila (CVE-2020-14498), que puede explotarse para lograr la ejecución remota de código.

Un atacante necesita engañar a las víctimas para que visiten un sitio web malicioso o abrir un correo electrónico malicioso que contenga un elemento HTML específicamente diseñado que desencadena la falla en eCatcher, y finalmente permite a los atacantes tomar el control completo de la máquina objetivo.

Los tres proveedores fueron notificados sobre las vulnerabilidades y respondieron rápidamente para lanzar soluciones de seguridad que corrijan las fallas de sus productos.

Se recomienda a los usuarios de Secomea que actualicen sus productos a las versiones liberadas de GateManager 9.2c/9.2i, los usuarios de Moxa deben actualizar EDR-G902/3 a la versión v5.5 mediante la aplicación de actualizaciones de firmware disponible para la serie EDR-G902 y EDR-G903. Los usuarios de HMS Networks también deberían actualizar eCatcher a la versión 6.5.5 o posterior.