Hackers están buscando activamente en Internet sistemas de control de acceso de puertas, con el fin de secuestrarlos y lanzar ataques DDoS, según informó la compañía de firewall SonicWall.

Los ataques cibernéticos están dirigidos a Linear eMerge E3, un producto de Nortek Security & Control (NSC).

Los dispositivos lineales eMerge E3 se encuentran en la categoría de hardware de *«sistemas de control de acceso»*. Se instalan en sedes corporativas, fábricas o parques industriales. Su principal propósito es controla a qué puertas y habitaciones pueden acceder los empleados y visitantes en función de sus credenciales o tarjetas inteligentes.

En mayo de 2019, investigadores de Applied Risk, una compañía de seguridad cibernética especializada en servicios de seguridad industrial, revelaron detalles acerca de diez vulnerabilidades que afectan a los dispositivos NSC Linear eMerge E3.

A pesar de que seis de las diez vulnerabilidades tenían un puntaje de gravedad de vulnerabilidad (CVSSv3) de 9.8 o 10 de un máximo de 10, NSC no pudo proporcionar parches, según un aviso de seguridad de Applied Risk.

Después de esto, Applied Risk lanzó un código de explotación de prueba de concepto en noviembre del mismo año.

Ahora, en un informe publicado la semana pasada, los investigadores de SonicWall afirman que los piratas informáticos están escaneando activamente Internet en busca de dispositivos NSC Linear eMerge E3 expuestos y utilizando una de las diez vulnerabilidades.

La vulnerabilidad en cuestión es CVE-2019-7256. Applied Risk describió la vulnerabilidad como una falla de inyección de comando. Es uno de los dos problemas que recibió un puntaje de 10 sobre 10, lo que significa que puede ser explotado a distancia, aún por atacantes poco calificados sin ningún conocimiento técnico avanzado.

> *«Este problema se desencadena debido a la desinfección insuficiente de las entradas proporcionadas por el usuario a una función PHP que permite la ejecución arbitraria de comandos con privilegios de root. Un atacante remoto no autenticado puede explotar esto para ejecutar comandos arbitrarios dentro del contexto de la aplicación, por medio de una solicitud HTTP diseñada»,* dijo SonicWall en una alerta de seguridad.

Los hackers utilizan la vulnerabilidad CVE-2019-7256 para hacerse cargo de los dispositivos, descargar e instalar malware y luego lanzar ataques DDoS en otros objetivos.

> *«Los atacantes parecen estar atacando activamente estos dispositivos, ya que vemos decenas de miles de visitas cada día, apuntando a más de 100 países con la mayoría de los ataques en Estados Unidos»*, dijo SonicWall.

Sin embargo, la superficie de ataque no es muy grande. SonicWall informó que el motor de búsqueda Shodan solo enumera *«2375 dispositivos eMerge con acceso a Internet».*

Este número es mucho más bajo que los millones de cámaras de seguridad y enrutadores domésticos que también están disponibles en línea. Sin embargo, la cantidad pequeña de dispositivos vulnerables no ha disuadido a los hackers hasta ahora, y es probable que los intentos de explotación sigan.

Si bien, hacer que su sistema de puerta de edificio inteligente inicie ataques DDoS en Steam o PlayStaton Network es un problema, una amenaza mayor es que estos sistemas vulnerables también se pueden usar como puntos de entrada a las redes internas de una organización.

En agosto del año pasado, Microsoft informó que observó a un equipo de piratas informáticos patrocinado por el estado ruso, que utilizaba dispositivos inteligentes de Internet de las Cosas (IoT) como puntos de lanzamiento para otros ataques en redes corporativas.

Los hackers rusos intentaron explotar un teléfono VoIP, una impresora de oficina y un decodificador de video, dijo Microsoft. Pero los dispositivos NCS Linear eMerge E3 son objetivos igualmente atractivos, principalmente debido a la alta gravedad de las diez vulnerabilidades reveladas el año pasado.

Se recomienda a los administradores de sistemas que trabajan con redes donde se instalan dispositivos NSC Linear eMerge E3, que retiren estos sistemas de Internet, o al menos, limiten el acceso a los dispositivos mediante un firewall o VPN.