La Agencia de Ciberseguridad y Seguridad de Infraestructura de los Estados Unidos (CISA) ha añadido una vulnerabilidad crítica ya corregida, que afecta a las puertas de enlace de acceso seguro de Array Networks AG y vxAG, a su catálogo de Vulnerabilidades Conocidas Explotadas (KEV). Esta actualización se produce tras informes de que dicha falla está siendo activamente utilizada en ataques en entornos reales.

Identificada como CVE-2023-28461 y con una puntuación CVSS de 9,8, la vulnerabilidad se origina en la ausencia de un mecanismo de autenticación adecuado, lo que permite a los atacantes ejecutar código arbitrario de forma remota. En marzo de 2023, el fabricante de hardware de redes lanzó una actualización (versión 9.4.0.484) para abordar este problema de seguridad.

> *«El fallo de ejecución remota de código en Array AG/vxAG es una vulnerabilidad que permite a un atacante acceder al sistema de archivos o ejecutar código de manera remota en la puerta de enlace SSL VPN utilizando el atributo `flags` en el encabezado HTTP, sin necesidad de autenticación. El producto puede ser comprometido a través de una URL específica»,* explicó Array Networks.

La inclusión en el catálogo KEV sigue al informe de la firma de ciberseguridad Trend Micro, que reveló que un grupo de ciberespionaje vinculado a China, conocido como Earth Kasha (también llamado MirrorFace), ha estado explotando vulnerabilidades en productos empresariales accesibles públicamente, como Array AG (CVE-2023-28461), Proself (CVE-2023-45727) y Fortinet FortiOS/FortiProxy (CVE-2023-27997), para lograr acceso inicial a sistemas.

Earth Kasha es conocido por sus extensivos ataques contra entidades en Japón, aunque en los últimos años también ha dirigido su atención a objetivos en Taiwán, India y Europa.

A principios de este mes, ESET informó sobre una campaña de Earth Kasha que tenía como objetivo a una entidad diplomática de la Unión Europea. Utilizaron un señuelo relacionado con la Exposición Universal 2025, que se celebrará en Osaka, Japón, a partir de abril de 2025,

para distribuir una puerta trasera conocida como ANEL.

Dado el uso activo de esta vulnerabilidad, se recomienda a las agencias del Poder Ejecutivo Civil Federal (FCEB) aplicar los parches correspondientes antes del 16 de diciembre de 2024 para proteger sus redes.

Además, se informó que al menos 15 grupos de hackers chinos, de un total de 60 actores de amenazas identificados, han estado implicados en la explotación de alguna de las 15 vulnerabilidades más comúnmente usadas en 2023, según el análisis de VulnCheck.

La compañía de ciberseguridad señaló que existen más de 440,000 dispositivos expuestos a internet que podrían ser vulnerables a ataques.

> *«Las organizaciones deben evaluar su exposición a estas tecnologías, mejorar la visibilidad de los riesgos potenciales, utilizar inteligencia de amenazas sólida, mantener prácticas robustas de gestión de parches e implementar controles de mitigación. Esto incluye limitar la exposición de estos dispositivos a internet siempre que sea posible»,* afirmó Patrick Garrity de VulnCheck.