La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA), publicó este jueves un Aviso de Sistemas de Control Industrial (ICSA) que advierte sobre múltiples vulnerabilidades en el equipo Mimosa de Airspan Networks, que podría permitir ser objeto de abuso para obtener la ejecución remota de código, crear una condición de denegación de servicio (DoS) y obtener información sensible.

> *«La explotación exitosa de estas vulnerabilidades podría permitir a un atacante obtener datos de usuario (incluyendo detalles de la organización) y otros datos confidenciales, comprometer la instancia EC2 en la nube de AWS (Amazon Web Services) de Mimosa y los cubos S3, y ejecutar código remoto no autorizado en todos los dispositivos Mimosa conectados a la nube»,* dijo CISA.

Las 7 vulnerabilidades, que fueron descubiertas e informadas a CISA por la compañía de seguridad cibernética industrial Claroty, afectan a los siguientes productos:

- Mimosa Management Platform (MMP) que ejecuta versiones anteriores a v1.0.3
- Punto a punto (PTP) C5c y C5x ejecutando versiones anteriores a v2.8.6.1
- Punto a multipunto (PTMP) A5x y Serie C (C5c, C5x y C6x) que ejecutan versiones anteriores a v2.5.4.1

La línea de productos Mimosa de Airspan Network ofrece soluciones de red híbrida de fibra inalámbrica (HFW) a proveedores de servicios, operadores industriales y gubernamentales para implementaciones de banda ancha de corto y largo alcance.

Los errores críticos son parte de siete vulnerabilidades totales, tres de las cuales tienen una calificación de 10 sobre 10 en la escala de gravedad de vulnerabilidad CVSS, lo que permite que un adversario ejecute código arbitrario, acceda a claves secretas e incluso modifique configuraciones.

Otras cuatro vulnerabilidades restantes podrían permitir que un atacante inyecte comandos arbitrarios, descifre contraseñas codificadas (pero no salted) y obtenga acceso no autorizado

a información confidencial.

Como medida de mitigación, se recomienda a los usuarios actualizar a MMP versión 1.0.4 o superior, PTP C5c y C5x versión 2.90 o superior, y PTMP A5x y C-series versión 2.9.0 o superior.

Además, CISA está atesorando a las organizaciones vulnerables para que minimicen la exposición de la red, aíslen las redes del sistema de control de la red empresarial y utilicen redes privadas virtuales (VPN) para el acceso remoto a fin de mitigar el riesgo de explotación de estas vulnerabilidades.

La divulgación también se produce cuando Cisco Talos publicó los detalles de una serie de vulnerabilidades críticas que Sealevel abordó en el dispositivo de borde conectado a WiFi SeaConnect 370W, que podría permitir que un atacante realice un ataque de intermediario (MiTM) y ejecute código remoto en el dispositivo de destino.