Un presunto intento de intrusión de ransomware contra un objetivo sin nombre aprovechó un dispositivo Mitel VoIP como punto de entrada para lograr la ejecución remota de código y obtener acceso inicial al entorno.

Estos hallazgos provienen de la compañía de seguridad cibernética CrowdStrike, que rastreó el origen del ataque hasta un dispositivo Mitel VoIP basado en Linux ubicado en el perímetro de la red, al mismo tiempo que identificó un exploit previamente desconocido, así como un par de medidas anti-forense adoptadas por el actor en el dispositivo para borrar los rastros de sus acciones.

El exploit de día cero es rastreado como CVE-2022-29499 y Mitel lo solucionó en abril de 2022 mediante un script de remediación que compartió con sus clientes. La vulnerabilidad tiene una calificación de gravedad de 9.8 en el sistema de calificación de vulnerabilidades CVSS, lo que la convierte en una deficiencia crítica.

> *«Se identificó una vulnerabilidad en el componente Mitel Service Appliance de MiVoice Connect (Mitel Appliances – SA 100, SA 400 y Virtual SA) que podría permitir a un atacante ejecutar código remoto (CVE-2022-29499) dentro del contexto del dispositivo de servicio»*, dijo la compañía.

El exploit implica dos solicitudes HTTP GET, que se usan para recuperar un recurso específico de un servidor, para desencadenar la ejecución remota de código al obtener comandos no autorizados de la infraestructura controlada por el atacante.

En el incidente investigado por CrowdStrike, el atacante parece haber usado el exploit para crear un shell inverso, utilizándolo para iniciar un shell web («pdf_import.php») en el dispositivo VoIP y descargar la herramienta proxy Chisel de código abierto.

Después, se ejecutó el binario, pero solo después de cambiarle el nombre a»memdump» en un intento de pasar desapercibido y utilizar la utilidad como un *«proxy inverso para permitir que el atacante se introdujera más en el entorno por medio del dispositivo VoIP»*. Pero la

detección posterior de la actividad detuvo su progreso y les impidió moverse lateralmente por medio de la red.

La divulgación llega menos de dos semanas después de que la compañía alemana de pruebas de penetración SySS revelara dos vulnerabilidades en los teléfonos de escritorio Mitel 800/6900 (CVE-2022-29854 y CVE-2022-29855) que, de ser explotadas exitosamente, podrían haber permitido a un hacker obtener privilegios de raíz en los dispositivos.

> *«La aplicación oportuna de parches es fundamental para proteger los dispositivos perimetrales. Sin embargo, cuando los actores de amenazas explotan una vulnerabilidad no documentada, la aplicación oportuna de parches se vuelve irrelevante»,* dijo Patrick Bennett, de CrowdStrike.

> *«Los activos críticos deben aislarse de los dispositivos perimetrales en la medida de lo posible. Idealmente, si un actor de amenazas compromete un dispositivo perimetral, no debería ser posible acceder a los activos críticos a través de 'un salto' desde el dispositivo comprometido».*

Actualización: Según el investigador de seguridad Kevin Beaumont, hay cerca de 21,500 dispositivos Mitel de acceso público en línea, la mayoría ubicados en Estados Unidos, seguidos por el Reino Unido, Canadá, Francia y Australia.