Se detectó que los hackers están abusando de un método de reflexión/amplificación de alto impacto para organizar ataques de denegación de servicio distribuido (DDoS) sostenido durante hasta 14 horas, con una tasa de amplificación sin precedentes de 4,294,967,296 a 1.

El vector de ataque, denominado TP240PhoneHome (CVE-2022-26143), ha sido armado para lanzar importantes ataques DDoS dirigidos a ISP de acceso de banda ancha, instituciones financieras, empresas de logística, empresas de juegos y otras organizaciones.

> *«Aproximadamente 2600 sistemas de colaboración Mitel MiCollab y MiVoice Business Express que actúan como puertas de enlace de PBX a Internet se implementaron incorrectamente con una instalación de prueba de sistema abusable expuesta al Internet público»,* dijo el investigador de Akamai, Chad Seaman en un aviso conjunto.

> *«Los atacantes estaban aprovechando activamente estos sistemas para lanzar ataques DDoS de reflexión/amplificación de más de 53 millones de paquetes por segundo (PPS)»,* agregó.

Los ataques de reflexión DDoS suelen implicar la suplantación de la dirección IP de una víctima para redirigir las respuestas de un objetivo, como un servidor DNS, NTP o CLDAP, de tal forma que las respuestas enviadas al remitente falsificado sean mucho más grandes que las solicitudes, lo que lleva a una inaccesibilidad total del servicio.

La primera señal de los ataques se detectó el 18 de febrero de 2022 utilizando los sistemas de colaboración MiCollab y MiVoice Business Express de Mitel como reflectores DDoS, esto como una respuesta de la exposición involuntaria de una instalación de prueba no autenticada a la Internet pública.

> *«Este vector de ataque en particular difiere de la mayoría de las metodologías de ataque de reflexión/amplificación UDP en que se puede abusar de la instalación de prueba del sistema expuesto para lanzar un ataque DDoS sostenido de hasta 14 horas de duración por medio de un solo paquete de inicio de ataque falsificado, lo que resulta en una relación de amplificación de paquetes récord de 4,294,967,296:1»,* dijo el investigador.

Específicamente, los ataques arman un controlador llamado tp240dvr («controlador TP-240») que está diseñado para escuchar comandos en el puerto UDP 100074 y *«no está destinado a estar expuesto a Internet. Es esta exposición a Internet que en última instancia permite que se abuse de él»,* dijo Akamai.

> *«El examen del binario tp240dvr revela que, debido a su diseño, un atacante teóricamente puede hacer que el servicio emita 2,147,483,647 respuestas a un solo comando malicioso. Cada respuesta genera dos paquetes en el cable, lo que lleva a aproximadamente 4,294,967,294 paquetes de ataque amplificados dirigidos hacia la víctima del ataque».*

En respuesta al descubrimiento, Mitel lanzó el martes actualizaciones de software que deshabilitan el acceso público a la función de prueba, al mismo tiempo que describen el problema como una vulnerabilidad de control de acceso que podría explotarse para obtener información confidencial.

> *«El impacto colateral de los ataques de reflexión/amplificación TP-240 es potencialmente significativo para las organizaciones con sistemas de colaboración Mitel MiCollab y MiVoice Business Express expuestos a Internet que se abusan como reflectores/amplificadores DDoS»,* dijo la compañía.

> *«Esto puede incluir la interrupción parcial o total de las comunicaciones de voz a través de estos sistemas, así como la interrupción adicional del servicio debido al consumo de capacidad de tránsito, el agotamiento de la tabla de estado de las traducciones de direcciones de red, los firewalls de estado, etcétera».*