Investigadores de ciberseguridad han revelado una falla crítica en la seguridad de la serie de teléfonos VoIP Grandstream GXP1600 que podría permitir a un atacante tomar el control de los dispositivos vulnerables.

La vulnerabilidad, identificada como CVE-2026-2329, posee una puntuación CVSS de 9.3 sobre un máximo de 10.0. Ha sido catalogada como un desbordamiento de búfer basado en pila sin autenticación, lo que podría derivar en la ejecución remota de código.

«Un atacante remoto puede aprovechar CVE-2026-2329 para lograr ejecución remota de código (RCE) sin autenticación y con privilegios de root en un dispositivo objetivo», afirmó el investigador de Rapid7 Stephen Fewer, quien descubrió y reportó el fallo el 6 de enero de 2026.

De acuerdo con la empresa de ciberseguridad Rapid7, el problema se origina en el servicio API web del dispositivo («/cgi-bin/api.values.get») y está disponible en la configuración predeterminada sin necesidad de autenticación.

Este endpoint está diseñado para obtener uno o varios valores de configuración del teléfono, como la versión del firmware o el modelo, mediante una cadena delimitada por dos puntos en el parámetro «request» (por ejemplo, «request=68:phone_model»). Posteriormente, dicha cadena se analiza para extraer cada identificador y añadirlo a un búfer de 64 bytes ubicado en la pila.

«Al añadir otro carácter al pequeño búfer de 64 bytes, no se realiza ninguna verificación de longitud para garantizar que no se escriban más de 63 caracteres (más el terminador nulo añadido) en este búfer», explicó Fewer. «Por lo tanto, un parámetro 'request' controlado por un atacante puede escribir más allá de los límites del pequeño búfer de 64 bytes en la pila, desbordándose hacia la memoria adyacente.»

Esto implica que un parámetro «request» malicioso, delimitado por dos puntos y enviado como parte de una solicitud HTTP al endpoint «/cgi-bin/api.values.get», puede provocar un desbordamiento de búfer en la pila. Como consecuencia, los actores malintencionados

podrían alterar el contenido de la pila y finalmente ejecutar código remoto en el sistema operativo subyacente.

La vulnerabilidad impacta a los modelos GXP1610, GXP1615, GXP1620, GXP1625, GXP1628 y GXP1630. El problema fue corregido mediante una actualización de firmware (versión 1.0.7.81) publicada a finales del mes pasado.

En un módulo de explotación de Metasploit desarrollado por Rapid7, se demostró que la falla puede explotarse para obtener privilegios de root en un dispositivo afectado y combinarse con un componente posterior a la explotación para extraer credenciales almacenadas en el equipo comprometido.

Además, la capacidad de ejecución remota de código puede utilizarse para reconfigurar el dispositivo objetivo y forzarlo a emplear un proxy malicioso del Protocolo de Inicio de Sesión (SIP), lo que permitiría al atacante interceptar llamadas entrantes y salientes, así como espiar conversaciones VoIP. Un proxy SIP actúa como servidor intermediario en redes VoIP para establecer y gestionar llamadas de voz o video entre terminales.

«No se trata de un exploit de un solo clic con fuegos artificiales y un mensaje de victoria», señaló Douglas McKee de Rapid7. «Sin embargo, la vulnerabilidad subyacente reduce la barrera de ataque de una manera que debería preocupar a cualquiera que opere estos dispositivos en entornos expuestos o con segmentación limitada.»