Zyxel lanzó actualizaciones de software para abordar dos vulnerabilidades de seguridad críticas que afectan a ciertos productos de firewall y VPN que podrían ser objeto de abuso por parte de atacantes remotos para lograr la ejecución de código.

Ambas vulnerabilidades, CVE-2023-33009 y CVE-2023-33010, son vulnerabilidades de desbordamiento de búfer y tienen una calificación de 9.8 sobre 10 en el sistema de puntuación CVSS.

Se puede observar una breve descripción de las vulnerabilidades a continuación:

- CVE-2023-33009: Vulnerabilidad de desbordamiento de búfer en la función de notificación, que podría permitir que un atacante no autenticado provoque una condición de denegación de servicio (DoS) y la ejecución remota de código.
- CVE-2023-33010: Vulnerabilidad de desbordamiento de búfer en la función de procesamiento de ID que podría permitir que un atacante no autenticado provoque una condición de denegación de servicio (DoS) y la ejecución remota de código.

Los siguientes dispositivos se ven afectados:

- ATP (versiones ZLD V4.32 a V5.36 parche 1, parcheado en ZLD V5.36 parche 2)
- USG FLEX (versiones ZLD V4.50 a V5.36 parche 1, parcheado en ZLD V5.36 parche 2)
- USG FLEX50(W) / USG20(W)-VPN (versiones ZLD V4.25 a V5.36 parche 1, parcheado en ZLD V5.36 parche 2)
- VPN (versiones ZLD V4.30 a V5.36 Parche 1, parcheado en ZLD V5.36 Parche 2), y
- ZyWALL/USG (versiones ZLD V4.25 a V4.73 Parche 1, parcheado en ZLD V4.73 Parche 2)

Se les atribuye el descubrimiento e informe de las vulnerabilidades a los investigadores de seguridad de TRAPA Security y STAR Labs SG.

El aviso llega menos de un mes después de que Zyxel enviara correcciones para otra vulnerabilidad de seguridad crítica en sus dispositivos de firewall, que podrían explotarse

para lograr la ejecución remota de código en los sistemas afectados.

El problema, rastreado como CVE-2023-28771 (puntuación CVSS: 9.8), también se le atribuyó a TRAPA Security, y el fabricante del equipo de red lo culpó al manejo inadecuado de mensajes de error. Desde entonces, ha estado bajo explotación activa por parte de atacantes asociados con la red de bots Mirai.