El fabricante de equipos de red Zyxel ha lanzado parches para una vulnerabilidad de seguridad crítica en sus dispositivos de firewall que podría explotarse para lograr la ejecución remota de código en los sistemas infectados.

La vulnerabilidad, rastreada como CVE-2023-28771, tiene una calificación de 9.8 en el sistema de puntuación CVSS. A los investigadores de TRAPA Security se les atribuyó el informe de la falla.

> *«El manejo inadecuado de mensajes de error en algunas versiones de firewall podría permitir que un atacante no autenticado ejecute algunos comandos del sistema operativo de forma remota mediante el envío de paquetes manipulados a un dispositivo afectado»,* dijo Zyxel en un aviso el 25 de abril de 2023.

Los productos afectados por la vulnerabilidad son:

- ATP (versiones ZLD V4.60 a V5.35, parcheado en ZLD V5.36)
- USG FLEX (versiones ZLD V4.60 a V5.35, parcheado en ZLD V5.36)
- VPN (versiones ZLD V4.60 a V5.35, parcheado en ZLD V5.36), y
- ZyWALL/USG (versiones ZLD V4.60 a V4.73, parcheado en ZLD V4.73 Parche 1)

Zyxel también abordó una vulnerabilidad de inyección de comando posterior a la autenticación de alta gravedad que afecta a versiones seleccionadas de firewall (CVE-2023-27991, puntuación CVSS: 8.8) que podría permitir que un atacante autenticado ejecute algunos comandos del sistema operativo remotamente.

La vulnerabilidad, que afecta a los dispositivos ATP, USG FLEX, USG FLEX 50(W)/USG20(W)-VPN y VPN, se resolvió en ZLD V5.36.

Finalmente, la compañía también envió correcciones para cinco vulnerabilidades de alta gravedad que afectan a varios firewalls y dispsitivos de punto de acceso (AP) (desde CVE-2023-22913 hasta CVE-2023-22918) que podrían resultar en la ejecución de código y

causar una condición de denegación de servicio (DoS).

Nikita Abramov, de la compañía rusa de seguridad cibernética Positive Technologies, fue acreditada por informar sobre los problemas. Abramov, a inicios del año, también descubrió cuatro vulnerabilidades de inyección de comandos y desbordamiento de búfer en CPE, ONT de fibra y extensores WiFi.

La vulnerabilidad más grave es CVE-2022-43389 (puntuación CVSS: 9.8), una vulnerabilidad de desbordamiento de búfer que afecta a los dispositivos CPE 5G NR/4G LTE.

> *«No requería autenticación para ser explotado y condujo a la ejecución de código arbitrario en el dispositivo. Como resultado, un atacante podría obtener acceso remoto al dispositivo y controlar completamente su funcionamiento»*, dijo Abramov.