Zyxel lanzó parches para abordar cuatro vulnerabilidades de seguridad que afectan a su firewall, controlador API y productos AP, para ejecutar comandos arbitrarios del sistema operativo y robar información seleccionada.

Las vulnerabilidades en cuestión son:

- CVE-2022-0734: Una vulnerabilidad de secuencias de comandos entre sitios (XSS) en algunas versiones de firewall que podría explotarse para acceder a información almacenada en el navegador del usuario, como cookies o tokens de sesión, a través de una secuencia de comandos maliciosa.
- CVE-2022-26531: Varias fallas de validación de entrada en los comandos de la interfaz de línea de comandos (CLI) para algunas versiones de firewall, controlador AP y dispositivos AP que podrían explotarse para provocar un bloqueo del sistema.
- CVE-2022-26532: Una vulnerabilidad de inyección de comandos en el comando CLI «packet-trace» para algunas versiones de firewall, controlador API y dispositivos AP que podría conducir a la ejecución de comandos arbitrarios del sistema operativo.
- CVE-2022-0910: Una vulnerabilidad de omisión de autenticación que afecta a versiones seleccionadas de cortafuegos y que podría permitir a un atacante pasar de la autenticación de dos factores a la autenticación de un factor a través de un cliente VPN IPsec.

Aunque Zyxel publicó parches de software par firewalls y dispositivos AP, la revisión para los controladores AP afectados por CVE-2022-26531 y CVE-2022-26532 solo se pueden obtener poniéndose en contacto con los respectivos equipos de soporte locales de Zyxel.

Este desarrollo se presenta como una vulnerabilidad crítica de inyección de comandos en versiones seleccionadas de los firewalls Zyxel (CVE-2022-30525, puntaje CVSS: 9.8) que ha sido objeto de explotación activa, lo que llevó a la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos a agregar el error a su Catálogo de Vulnerabilidades Explotadas Conocidas.