Zyxel lanzó un parche para abordar una vulnerabilidad crítica en su firmware con respecto a una cuenta secreta no documentada y codificada que podría ser abusada por un atacante para iniciar sesión con privilegios administrativos y comprometer sus dispositivos de red.

La vulnerabilidad, rastreada como CVE-2020-29583 y con puntuación CVSS de 7.8, afecta a la versión 4.60 presente en una amplia gama de dispositivos Zyxel, incluidos Unified Security Gateway (USG), USG FLEX, ATP y productos de firewall VPN.

Niels Teusink, investigador de EYE, informó la vulnerabilidad a Zyxel el 29 de noviembre, por lo que la compañía lanzó un parche de firmware (ZLD V4.60 Patch 1) el 18 de diciembre.

Según el aviso publicado por Zyxel, la cuenta indocumentada «zyfwp» viene con una contraseña que no se puede cambiar («PrOw! AN_fXp») que no solo se almacena en texto plano, sino que también podría ser utilizada por un tercero malintencionado para iniciar sesión en SSH o interfaz web con privilegios de administrador.

Zyxel dijo que las credenciales codificadas se implementaron para entregar actualizaciones de firmware automáticas a los puntos de acceso conectados a través de FTP.

Al asegurar que al rededor del 10% de los 1000 dispositivos en los Países Bajos ejecutan la versión de firmware afectada, Teusink dijo que la relativa facilidad de explotación de la falla la convierte en una vulnerabilidad crítica.

> *«Como el usuario 'zyfwp' tiene privilegios de administrador, esta es una vulnerabilidad grave. Un atacante podría comprometer completamente la confidencialidad, integridad y disponibilidad del dispositivo»,* dijo Teusink.
>
> *«Alguien podría, por ejemplo, cambiar la configuración del firewall para permitir o bloquear cierto tráfico. También podría interceptar el tráfico o crear cuentas VPN para obtener acceso a la red detrás del dispositivo. Combinado con una vulnerabilidad como Zerologon, esto podría ser devastador para las pequeñas y*

> *medianas empresas».*

También se espera que la compañía taiwanesa aborde el problema en sus controladores de punto de acceso (AP) con un parche V6.10 que se lanzará en abril de 2021.