La Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos agregó el lunes dos vulnerabilidades de seguridad, incluyendo el error de ejecución remota de código recientemente revelado, que afecta a los firewalls Zyxel, a su Catálogo de Vulnerabilidades Explotadas Conocidas, citando evidencia de explotación activa.

Rastreada como CVE-2022-30535, la vulnerabilidad tiene una clasificación de gravedad de 9.8 y se relaciona con una vulnerabilidad de inyección de comandos en versiones seleccionadas del firewall Zyxel, que podría permitir que un adversario no autenticado ejecute comandos arbitrarios en el sistema operativo subyacente.

Los dispositivos afectados incluyen:

- USG FLEX 100, 100 W, 200, 500, 700
- USG20-VPN, USG20W-VPN
- ATP 100, 200, 500, 700, 800
- Serie VPN

El problema, para el cual la compañía taiwanesa lanzó parches a fines de abril (ZLD V5.30), se hizo público el 12 de mayo luego de un proceso de divulgación coordinado con Rapid7.

Un día después, la Fundación Shadowserver, dijo que comenzó a detectar intentos de explotación, con la mayoría de los dispositivos vulnerables ubicados en Francia, Italia, Estados Unidos, Suiza y Rusia.

CISA también agregó al catálogo CVE-2022-22947, otra vulnerabilidad de inyección de código en Spring Cloug Gateway, que podría explotarse para permitir la ejecución remota arbitraria en un host remoto mediante una solicitud especialmente diseñada.

La vulnerabilidad tiene una calificación de 10 y desde entonces, se ha abordado en las versiones 3.1.1 o posterior de Spring Cloud Gateway y 3.0.7 o posterior a partir de marzo de 2022.