Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00640-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	17 de mayo de 2022
Última revisión	17 de mayo de 2022

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT de Gobierno, comparte información sobre una vulnerabilidad que afecta a dispositivos VPN y firewalls Zyxel.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidad

CVE-2022-30525

Impacto

Vulnerabilidad crítica

CVE-2022-30525: Su explotación exitosa permite a un atacante remoto la inyección de comandos arbitrarios sin autenticación.

Productos afectados

USG FLEX 100(W), 200, 500, 700, versiones firmware ZLD V5.00 a ZLD V5.21 Patch 1.
USG FLEX 50(W) / USG20(W)-VPN, versiones firmware ZLD V5.10 a ZLD V5.21 Patch 1.
ATP series, versiones firmware ZLD V5.10 a ZLD V5.21 Patch 1.
VPN series, versiones firmware ZLD V4.60 through ZLD V5.21 Patch 1.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.
Parche ZLD V5.30.

Enlaces

https://www.zyxel.com/support/Zyxel-security-advisory-for-OS-command-injection-vulnerability-of-firewalls.shtml
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30525