Alerta de seguridad cibernética	9VSA23-00838-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	25 de mayo de 2023
Última revisión	25 de mayo de 2023

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 CSIRT de Gobierno comparte información de dos vulnerabilidades críticas que afectan a varios productos de firewall y VPN de Zyxel, que han sido parchadas por la compañía.

Vulnerabilidades

CVE-2023-33009 y CVE-2023-33010

Impacto

Vulnerabilidades críticas

CVE-2023-33009 y CVE-2023-33010: Vulnerabilidad de desbordamiento de buffer en la función de notificación en algunos productos de Zyxel, permitiendo a un atacante no autenticado llevar a cabo de ejecución remota de código o imponer condiciones de denegación de servicio (DoS).

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

Zyxel ATP firmware versiones ZLD V4.32 a V5.36 Patch 1 (parchado en ZLD V5.36 Patch 2)
Zyxel USG FLEX firmware versiones ZLD V4.50 a V5.36 Patch 1 (parchado en ZLD V5.36 Patch 2)
Zyxel USG FLEX50(W) / USG20(W)-VPN firmware versiones ZLD V4.25 a V5.36 Patch 1 (parchado en ZLD V5.36 Patch 2)
Zyxel VPN firmware versiones ZLD V4.30 a V5.36 Patch 1 (parchado en ZLD V5.36 Patch 2)
Zyxel ZyWALL/USG firmware versiones ZLD V4.25 a V4.73 Patch 1 (parchado en ZLD V4.73 Patch 2)

Enlaces

http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-multiple-buffer-overflow-vulnerabilities-of-firewalls

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33009

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-33010

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.05.25 10:26:00 -04'00'