Zyxel, la compañía fabricante de equipos de red, lanzó actualizaciones de seguridad para una vulnerabilidad crítica que afecta a algunos de sus productos de firewall y VPN comerciales, que podría permitir que un atacante tome el control de los dispositivos.

> *«Se ha encontrado una vulnerabilidad de omisión de autenticación causada por la falta de un mecanismo de control de acceso adecuado en el programa CGI de algunas versiones de firewall. La falla podría permitir a un atacante eludir la autenticación y obtener acceso administrativo al dispositivo»,* dijo la compañía.

La vulnerabilidad se rastrea como CVE-2022-0342 y tiene una calificación CVSS de 9.8. Alessandro Sgreccia, de Tecnical Service Srl, Roberto García H y Victor García R, de Innotec Security, fueron acreditados por reportar el error.

Los productos afectados de Zyxel son:

- USG/ZyWALL ejecutando versiones de firmware ZLD V4.20 a ZLD V4.70 (corregido en ZLD V4.71).
- USG FLEX con versiones de firmware ZLD V4.50 a ZLD V5.20 (corregido en ZLD V5.21 Parche 1).
- ATP con versiones de firmware ZLD V4.32 a ZLD V5.20 (corregido en ZLD V5.21 Parche 1).
- VPN con versiones de firmware ZLD V4.30 a ZLD V5.20 (corregido en ZLD V5.21).
- NSG que ejecuta las versiones de firmware V1.20 a V1.33 Parche 4 (Hotfix V1.33p4_WK11 disponible ahora, con el parche estándar V1.33 Parche 4 esperado en mayo de 2022).

Aunque no existe evidencia de que la vulnerabilidad haya sido explotada en la naturaleza, se recomienda que los usuarios instalen las actualizaciones de firmware para evitar posibles amenazas.

CISA advierte sobre vulnerabilidades de Sophos y Trend Micro explotadas activamente

La divulgación se produce cuando Sophos y SonicWall lanzaron parches esta semana para sus dispositivos de firewall para resolver vulnerabilidades críticas (CVE-2022-1040 y CVE-2022-22274), que podrían permitir que un atacante remoto ejecute código arbitrario en los sistemas afectados.

La vulnerabilidad crítica del firewall de Sophos, que se observó explotada en ataques activos contra organizaciones selectas en el sur de Asia, fue agregada desde entonces por la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA) a su Catálogo de Vulnerabilidades Explotadas Conocidas.

También se agregó a la lista una vulnerabilidad de carga de archivos arbitrarios de alta gravedad en el producto Apex Central de Trend Micro, que podría permitir que un atacante remoto no autenticado cargue un archivo arbitrario, lo que resultaría en la ejecución de código (CVE-2022-26871, puntaje CVSS: 8.6).

> *«Trend Micro observó un intento activo de explotación contra esta vulnerabilidad en estado salvaje (ITW) en un número muy limitado de instancias, y ya hemos estado en contacto con estos clientes. Se recomienda encarecidamente a todos los clientes que actualicen a la última versión lo antes posible»,* dijo la compañía.