La Agencia de Ciberseguridad e Infraestructura de EE. UU. (CISA) incluyó varias vulnerabilidades de seguridad que afectan productos de Zyxel, North Grid Proself, ProjectSend y CyberPanel en su catálogo de Vulnerabilidades Conocidas Explotadas (KEV), basándose en pruebas de que estas están siendo activamente explotadas.

Las vulnerabilidades identificadas son las siguientes:

- CVE-2024-51378 (puntuación CVSS: 10.0): una vulnerabilidad de permisos predeterminados incorrectos que posibilita eludir la autenticación y ejecutar comandos arbitrarios usando metacaracteres de shell en la propiedad *statusfile*.
- CVE-2023-45727 (puntuación CVSS: 7.5): una falla en la restricción de referencias de Entidades Externas XML (XXE), que podría permitir a un atacante remoto y no autenticado realizar un ataque XXE.
- CVE-2024-11680 (puntuación CVSS: 9.8): una vulnerabilidad de autenticación inadecuada que permite a un atacante remoto y no autenticado crear cuentas, cargar *web shells* y ejecutar JavaScript malicioso.
- CVE-2024-11667 (puntuación CVSS: 7.5): una vulnerabilidad de recorrido de rutas en la interfaz de administración web, que podría permitir a un atacante descargar o cargar archivos mediante una URL manipulada.

La inclusión de CVE-2023-45727 en el catálogo KEV se dio tras la publicación de un informe de Trend Micro el 19 de noviembre de 2024, que vinculó su explotación activa a un grupo de ciberespionaje relacionado con China llamado Earth Kasha (también conocido como MirrorFace).

Además, la semana pasada, la empresa de ciberseguridad VulnCheck reveló que actores maliciosos han intentado aprovechar la CVE-2024-11680 desde septiembre de 2024 para ejecutar cargas útiles posteriores a la explotación.

Por otro lado, el uso de CVE-2024-51378 y CVE-2024-11667 ha sido asociado con diversas campañas de ransomware, como PSAUX y Helldown, según Censys y Sekoia.

Se recomienda a las agencias del Ramo Ejecutivo Civil Federal (FCEB) que resuelvan las vulnerabilidades detectadas antes del 25 de diciembre de 2024 para proteger sus redes.

Varias vulnerabilidades en routers I-O DATA bajo ataque

Este nuevo anuncio se produce después de que JPCERT/CC alertara sobre tres fallas de seguridad en los routers I-O DATA UD-LT1 y UD-LT1/EX, que están siendo aprovechadas por actores de amenazas desconocidos.

- CVE-2024-45841 (puntuación CVSS: 6.5): una vulnerabilidad de asignación incorrecta de permisos para recursos clave, que permite a un atacante con acceso a una cuenta de invitado leer archivos sensibles, incluidos aquellos que contienen credenciales.
- CVE-2024-47133 (puntuación CVSS: 7.2): una vulnerabilidad de inyección de comandos en el sistema operativo (OS) que permite a un usuario autenticado con privilegios administrativos ejecutar comandos arbitrarios.
- CVE-2024-52564 (puntuación CVSS: 7.5): una vulnerabilidad de inclusión de características no documentadas, que permite a un atacante remoto desactivar el firewall, ejecutar comandos arbitrarios del sistema o modificar la configuración del router.

Si bien ya se ha lanzado una actualización para la CVE-2024-52564 en el firmware Ver2.1.9, se espera que las correcciones para las otras dos vulnerabilidades se publiquen el 18 de diciembre de 2024 (Ver2.2.0).

Mientras tanto, la compañía japonesa ha recomendado a sus clientes que limiten la exposición de la pantalla de configuración a internet desactivando la administración remota, cambiando las contraseñas predeterminadas de los usuarios invitados y asegurándose de que las contraseñas de los administradores no sean fáciles de adivinar.