Zyxel ha publicado actualizaciones de seguridad para corregir fallos críticos que afectan a dos de sus dispositivos de almacenamiento conectado a la red (NAS), los cuales ya han alcanzado el estado de fin de vida útil (EoL).

La explotación exitosa de tres de las cinco vulnerabilidades podría permitir a un atacante no autenticado ejecutar comandos del sistema operativo (OS) y código arbitrario en las instalaciones afectadas.

Los modelos impactados incluyen NAS326 con versiones V5.21(AAZF.16)C0 y anteriores, y NAS542 con versiones V5.21(ABAG.13)C0 y anteriores. Estos problemas se han solucionado en las versiones V5.21(AAZF.17)C0 y V5.21(ABAG.14)C0, respectivamente.

Aquí se detalla brevemente cada una de las fallas:

- CVE-2024-29972: Una vulnerabilidad de inyección de comandos en el programa CGI «remote_help-cgi» que podría permitir a un atacante no autenticado ejecutar ciertos comandos del sistema operativo (OS) al enviar una solicitud HTTP POST manipulada.
- CVE-2024-29973: Una vulnerabilidad de inyección de comandos en el parámetro 'setCookie' que podría permitir a un atacante no autenticado ejecutar algunos comandos del OS al enviar una solicitud HTTP POST manipulada.
- CVE-2024-29974: Una vulnerabilidad de ejecución remota de código en el programa CGI 'file_upload-cgi' que podría permitir a un atacante no autenticado ejecutar código arbitrario cargando un archivo de configuración manipulado.
- CVE-2024-29975: Una vulnerabilidad de gestión inadecuada de privilegios en el binario ejecutable SUID que podría permitir a un atacante local autenticado con privilegios de administrador ejecutar ciertos comandos del sistema como usuario 'root'.
- CVE-2024-29976: Una vulnerabilidad de gestión inadecuada de privilegios en el comando 'show_allsessions' que podría permitir a un atacante autenticado obtener información de la sesión de un administrador conectado, incluyendo cookies en un dispositivo afectado.

El investigador de seguridad de Outpost24, Timothy Hjort, ha sido acreditado con el

descubrimiento y reporte de las cinco vulnerabilidades. Es importante mencionar que dos de las fallas de escalación de privilegios que requieren autenticación aún no han sido parcheadas.

Aunque no hay pruebas de que estos problemas hayan sido explotados en entornos reales, se recomienda a los usuarios actualizar a la versión más reciente para una protección óptima.