Aviso adicional sobre la vulnerabilidad de seguridad descubierta en las impresoras CL4/6NX Plus

04/08/2025

SATO Europa

Resumen

Además de las vulnerabilidades identificadas anteriormente (CWE-22, CWE-287 y CWE-863), se han confirmado dos nuevas vulnerabilidades: CWE-78 y CWE-434.

Ya se han aplicado las contramedidas adecuadas para estos problemas recientemente identificados.

Para obtener más detalles, consulte las secciones a continuación tituladas [Solución] o [Solución alternativa].

Para preguntas y consultas, complete nuestro formulario de contacto aquí.

Vulnerabilidad de seguridad descubierta en impresoras CL4/6NX Plus

04/08/2025

SATO Europa

Resumen

Se descubrió que algunas impresoras de etiquetas SATO tenían vulnerabilidades relacionadas con la autorización incorrecta (CWE-863, CWE-287) y el recorrido de ruta (CWE-22) que pueden conducir a cambios de configuración no autorizados y manipulación de archivos, lo que podría afectar el funcionamiento de las impresoras.

No se conocen casos de explotación de estas vulnerabilidades, y los usuarios de impresoras no corren el riesgo de manipulación de datos o exposición de información siempre que los usuarios tomen medidas para proteger sus sistemas del acceso no autorizado. Sin embargo, recomendamos a los usuarios que apliquen la siguiente solución a sus impresoras para mejorar la seguridad.

Impresoras afectadas

- CL4/6NX Plus
- CL4/6NX-J Plus (modelo de Japón)

Solución

Estamos lanzando una nueva actualización de firmware de la impresora para parchear las vulnerabilidades. Para obtener información sobre la actualización del firmware, póngase en contacto con su representante de SATO más cercano o con el distribuidor donde compró la impresora. Póngase en contacto con nosotros para concertar una cita.

Solución alternativa

Los usuarios pueden solucionar las vulnerabilidades habilitando el firewall de la impresora y deshabilitando la función WebConfig, si no puede tener instalada la actualización de firmware debido a ciertas razones técnicas. Tenga en cuenta que la solución alternativa es temporal y que, idealmente, debería remediar las vulnerabilidades a través del parche de seguridad una vez que su situación lo permita.

・Siga los pasos a continuación para aplicar la solución alternativa. También puede consultar la sección "Varias configuraciones del producto" en nuestro manual de usuario en línea para obtener más información.

Habilitar firewall

Vaya al menú Configuración de la impresora y haga clic en Interfaz> Red> Avanzado> Firewall> Habilitar.

Deshabilitar WebConfig (función para ver o cambiar la configuración de la impresora a través del navegador web)

Vaya al menú Configuración de la impresora y haga clic en Interfaz> Red> Avanzado>

Firewall> Permitir servicios y puertos> WebConfig> Desactivar.

Para preguntas y consultas, complete nuestro formulario de contacto aquí.