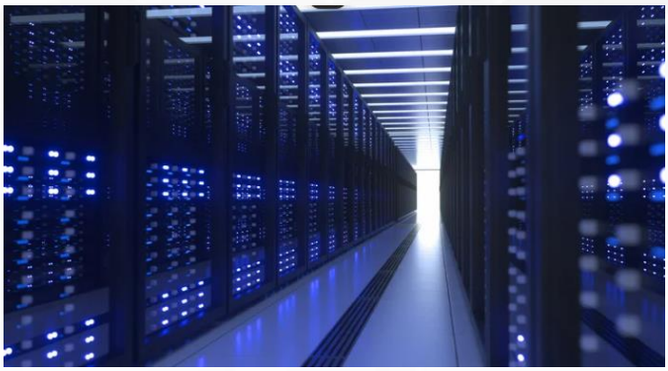
ALERTA

Infraestructuras Críticas

[COLCERT AL-0612-031]

TLP:CLEAR

ICCN



”Se lanzaron 14 avisos de seguridad que abordaron 120 vulnerabilidades de terceros”

El martes de parches de junio de 2024, trajo consigo una serie de avisos de seguridad críticos para sistemas de control industrial (ICS) por parte de diversos proveedores, incluyendo Siemens, Schneider Electric, Aveva y la Agencia de Seguridad de Infraestructura y Ciberseguridad de los Estados Unidos (CISA).

Resumen

Estos avisos detallan varias vulnerabilidades que podrían ser explotadas por actores malintencionados para tomar el control de sistemas industriales críticos o interrumpir su operación.

Impacto en seguridad digital

Las vulnerabilidades notables incluyen una falla crítica de omisión de autenticación en el software PowerSys y vulnerabilidades de ejecución de código en varios productos.
Se resolvieron vulnerabilidades en dispositivos Simatic S7-200 y Sinec Traffic Analyzer.

Para protegerse contra estas vulnerabilidades

Se recomienda a los usuarios de sistemas ICS que revisen los avisos de seguridad publicados por los proveedores relevantes e implementen las actualizaciones de seguridad correspondientes de manera oportuna.Implementar medidas de seguridad en profundidad, como segmentación de redes, control de acceso y monitoreo de seguridad, para reducir la superficie de ataque y detectar actividades maliciosas.

Establecer planes de respuesta a incidentes y realizar pruebas de recuperación de desastres para minimizar el impacto de posibles ataques cibernéticos.

NIVEL DE RIESGO

MEDIO

FUENTES:

1. https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp https://www.aveva.com/en/support-and-success/cyber-security-updates/
2. https://www.cisa.gov/news-events/cybersecurity-advisories
3. https://www.securityweek.com/ics-patch-tuesday-advisories-published-by-siemens-schneider-electric-aveva-cisa/

COLCERT