BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-33
Fecha de publicación: 13/09/2024
Tema: Vulnerabilidad Crítica en Sistemas Industriales Siemens
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- SIMATIC Process Historian versión anterior a V9.2.
- SIMATIC PCS 7 versiones anteriores a V9.1 SP2
- SIMATIC WinCC versión anterior a V7.5 SP2 Update 18.
- SIMATIC BATCH: Todas las versiones previas a la actualización están afectadas.
- SIMATIC Information Server versión anterior a V2020.

Descripción

Siemens publicó un comunicado sobre la vulnerabilidad CVE-2024-35783, una falla crítica con una puntuación de 9.4 en el CVSS. Esta vulnerabilidad afecta a sistemas industriales clave como SIMATIC PCS 7, SIMATIC Process Historian, y SIMATIC WinCC y permite que un atacante autenticado ejecute comandos arbitrarios, comprometiendo potencialmente la integridad de sistemas de control industrial críticos

La vulnerabilidad surge por el manejo inadecuado de privilegios en el servidor de bases de datos. En configuraciones específicas, el servidor puede ejecutarse con privilegios elevados, lo que permitiría a un atacante obtener control administrativo sobre los sistemas afectados, comprometiendo datos y alarmas críticas en los entornos industriales

Solución

Para solucionar este fallo se debe actualizar las versiones más recientes disponibles. Siemens ha emitido parches para algunos productos, como SIMATIC PCS 7, que debe actualizarse a WinCC V7.5 SP2 Update 18 o superior. Para otros productos como SIMATIC Process Historian y SIMATIC WinCC, aún se esperan parches, por lo que se recomienda aplicar las medidas de mitigación proporcionadas por Siemens.
Para más detalles y actualizaciones, visita el siguiente enlace: https://cert-portal.siemens.com/productcert/html/ssa-629254.html

Información adicional:

- https://securityonline.info/cve-2024-35783-cvss-9-4-critical-severity-flaw-exposes-siemens-industrial-systems/
- https://news.backbox.org/2024/09/13/critical-severity-flaw-exposes-siemens-industrial-systems/

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com