



## ALERTA

### Parcheo a vulnerabilidades en operación crítica

COLCERT AL-1411-055

Schneider Electric ha emitido una alerta de seguridad sobre vulnerabilidades críticas encontradas en sus Controladores Lógicos Programables (PLC) Modicon M340, Momentum y MC80, (CVE-2024-8936, CVE-2024-8937 y CVE-2024-8938) utilizados comúnmente en entornos industriales. Estas vulnerabilidades podrían permitir a los atacantes acceder en los sistemas de forma no autorizada.

### ELEMENTOS DE INTELIGENCIA DISPONIBLES

De manera adicional también se indica que manipular la memoria y ejecutar código malicioso, pueden ocasionar pérdida de datos, interrupciones en los procesos y otros daños graves. Schneider Electric ha lanzado parches de seguridad y ha recomendado medidas de mitigación adicionales para proteger estos sistemas.



#### ANÁLISIS



**Vulnerabilidades Críticas:** Se han identificado múltiples vulnerabilidades en los PLC de Schneider Electric, incluyendo problemas de validación de entrada, desbordamientos de búfer y otras debilidades que podrían ser explotadas por atacantes.

**Impacto Severo:** Las consecuencias de explotar estas vulnerabilidades pueden ser graves, incluyendo el acceso no autorizado a sistemas industriales, la manipulación de procesos y la interrupción de operaciones críticas.

### IMPACTO PARA COLOMBIA Y LA REGIÓN

Las vulnerabilidades descubiertas en los PLC de Schneider Electric subrayan la importancia de mantener actualizados los sistemas industriales y de implementar medidas de seguridad robustas para protegerlos de ciberataques.

Las organizaciones que utilizan estos dispositivos deben tomar medidas inmediatas para mitigar estos riesgos y proteger sus operaciones.

### NIVEL DE RIESGO

MEDIO

#### FUENTES:

<https://download.schneider-electric.com/doc/SEVD-2024-317-03/SEVD-2024-317-03.pdf>

<https://securityonline.info/schneider-electric-warns-of-multiple-vulnerabilities-in-modicon-controllers/>



COLCERT