06/12/2013

EPR/18/013

www.enisa.europa.eu

ENISA, la agencia de ciberseguridad de la UE, apuesta por una mayor protección de los sistemas SCADA.

Ante la pregunta «¿Durante cuánto tiempo podremos mantener unas infraestructuras críticas que usan sistemas SCADA sin parchear?», ENISA, la agencia de ciberseguridad de la UE, sostiene que la UE y sus Estados miembros podrían organizar con anticipación la gestión de parches a fin de mejorar la seguridad de los sistemas SCADA.

La mayor parte de las infraestructuras críticas de Europa pertenecen a sectores tales como el de la energía, el transporte y el suministro de agua. Estas infraestructuras están en su mayor parte gestionadas y controladas por Sistemas de Supervisión para el Control y la Obtención de Datos (SCADA, por sus siglas en inglés), los cuales constituyen a su vez un subgrupo de Sistemas de Control Industrial (ICS, por sus siglas en inglés). Durante la última década, la tecnología SCADA ha pasado de estar compuesta por sistemas aislados a disponer de una arquitectura abierta y unas tecnologías estándar, altamente interconectadas con otras redes de empresa y con Internet.

- Una consecuencia de esta transformación es la mayor vulnerabilidad a ataques exteriores. Para optimizar la seguridad de los sistemas SCADA se pueden aplicar parches.
- En estos momentos, dos de los principales problemas en relación con el parcheado son el índice de error en los parches (60%)[1] y la falta de parches: menos del 50% de las 364 vulnerabilidades públicas tenían parches[2] disponibles para los sistemas SCADA.

  De las buenas prácticas y recomendaciones que pueden mejorar el estado de la seguridad de los entornos SCADA, cabría destacar las siguientes:
- Controles de compensación:
  - Incremento en la defensa de profundidad a través de la segmentación de la red para crear zonas de confianza que se comuniquen mediante el uso de controles de acceso;
  - Fortalecimiento de los sistemas SCADA mediante la eliminación de funciones innecesarias;
  - Uso de técnicas como la aplicación de listas blancas y la inspección profunda de paquetes.
- Programa de gestión de parches y contrato de servicio:
  - Los propietarios de los equipos también deberían establecer un contrato de servicio de gestión de parches para definir las responsabilidades tanto del proveedor como del cliente en el proceso de gestión de parches;
  - Los propietarios de los equipos siempre deberían realizar sus propias pruebas. Esto puede llevarse a cabo virtualmente o bien manteniendo sistemas de pruebas por separado;
  - Los sistemas certificados deberían volverse a certificar después de haberse aplicado un parche.

[1] *«En 2011, los ICS-CERT observaron un índice de error del 60% en parches que reparaban los casos de vulnerabilidad denunciados en los productos de sistemas de control». (Kevin Hemsley – ICS-CERT)*

[2] *«Menos del 50% de las 364 vulnerabilidades públicas registradas por los ICS-CERT contaban con parches disponibles». (SCADA Security Scientific Symposium (S4), enero de 2012, McBride)*

El Profesor Udo Helmbrecht, Director Ejecutivo de ENISA, comentó: «*Aunque la gestión de parches no es una solución milagrosa que resolverá los problemas de seguridad de los sistemas SCADA, sí que es importante que las organizaciones establezcan una política de gestión de parches. La Unión Europea o sus Estados miembros podrían avanzar en la sensibilización con respecto a los parches implementando una gestión de parches siempre que se establezcan nuevos requisitos para dispositivos».*

Informe completo

Contexto: Estrategia de ciberseguridad de la UE.

Entrevistas: Ulf Bergstrom, portavoz, ulf.bergstrom@enisa.europa.eu, móvil: + 30 6948 460 143, o Adrian Pauna, Experto, adrian.pauna@enisa.europa.eu

Traducción. La versión original en inglés es el documento auténtico.
www.enisa.europa.eu