Vulnerabilities In Industrial Control System

Cyber criminals tend to target common loopholes or vulnerabilities in Industrial Control Systems (ICS). Here are some vulnerabilities found in ICS:

Weak User Authentication

Authentication is required to prove the identity of the users on a network. A weak user authentication system with out-of-date management & policies can be easily breached or bypassed.

Buffer Overflows

They are programming errors that result in overriding of data in memory blocks adjacent to the block in which software code is stored. This crashes the program, corrupts data or allows malicious code in the system resulting in a cyber attack.

Poor Adoption Of Software

Improper set-up of untested software and faulty implementation of patches can result in backdoors in ICS set up which can be exploited by cyber criminals. Thus, verify the functioning and regulatory requirements before implementing a software.

Improper Password Management

Poor password management for ICS is a common vulnerability. It is important to adopt stringent password management techniques like identity-based systems that use biometric verification.

www.centextech.com

Centex Technologies

CENTEX TECHNOLOGIES

13355 Noel Road, Suite # 1100, Dallas, TX 75240

Phone: (972) 375 - 9654

501 N. 4th Street, Killeen, TX - 76541

Phone: (254) 213 - 4740

1201 Peachtree St NE, Suite 200, Atlanta, GA 30361

Phone: (404) 994 - 5074

7600 Chevy Chase Drive, Suite 300,Austin, TX 78752

Phone: (512) 956 - 5454