ICS-CERT ADVISORY

ICSA-10-228-01 — VENDOR ADMIN ACCOUNTS WARNING

AUGUST 16, 2010

OVERVIEW

An asset owner recently notified the ICS-CERT that a vendor support contractor had added an administrative-level account during installation of new control systems software. The support contractor intended the account to be the default used to train their people for all future work on those systems. The addition of an administrative account to an ICS network with the password known by a contract company increases the cybersecurity risk to the asset owner.

This advisory highlights existing practices that may adversely impact the cybersecurity of industrial control systems (ICS) environments relative to malicious actors.

IMPACT

All control systems maintained by vendors, integrators, or other contractors can potentially be impacted by the practice of adding “back door” administrative accounts for future access to perform maintenance, updates, or training.

The impact to individual sites may vary, but the potential exists for an administrator-level username and password used by support personnel to be known to multiple individuals outside the owner’s organization and to be undocumented within the owner’s security policy framework. This essentially creates a backdoor into each system serviced by the support contractor and may not be recorded in the system’s configuration management process.

BACKGROUND

Third-party support contractors cannot always predict the challenges they will encounter during on site service work. As a result, contract service organizations often train their field staff to create and use a specific account with administrator privileges. This allows them to access the system to troubleshoot and to install, uninstall, or patch software components as needed. Generally, the goal is to increase productivity and ease of maintenance; however, this access may circumvent the asset owner’s user-account policies, contracting requirements, or user agreements.

MITIGATION

The possibility exists that asset owners may not have been notified by their contractors of such practices and therefore, are advised to audit their systems for back door administrative accounts. Asset owners should also discuss procedures with their vendor or service organizations and voice their concerns for the security impacts of creating additional user accounts with administrative privileges. This includes, as needed, alternative practices and a pre-set understanding of the work that will be performed. The Department of Homeland Security (DHS) provides guidance in the document *Cyber Security Procurement Language for Control Systems* for developing cybersecurity-related contractual requirements for control system work. This document is currently available at http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_100809.pdf.

Where it is not possible or practical to avoid creating an administrator account (some control system software versions may require this practice) the asset owner should work with the contractor or vendor service organization to reach agreement on how best to control the system's cybersecurity risk profile. This should be formalized into a security level agreement that clearly defines the responsibilities of both parties and should be documented in the systems configuration management process.

Asset owners and vendor organizations should follow their established internal procedures if any suspected malicious activity is observed and report their findings to ICS-CERT for tracking and correlation against other incidents. ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For Control System Security Program Information and Incident Reporting:
www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.