INDUSTRIAL
CONTROL
SYSTEMS
Community of Interest

Vulnerability Management in Industrial Control System / Operational Technology Environments - Meet Admin Corp

Introduction

This article is designed to be read in conjunction with the ICS COI guidance article - Vulnerability Management in Industrial Control Systems / Operational Technology Environments, in addition to NCSC's principle based vulnerability management guidance.

If you are responsible for the management or maintenance of Industrial Control System (ICS) /Operational Technology (OT) assets, this article is designed to support you in adopting a mature vulnerability management process that covers ICS/OT environments. This article covers elements of maintaining awareness of vulnerabilities in your systems, prioritising their remediation and if needed make a case to management for a shutdown. It also covers elements of how vulnerabilities within legacy technology often found in ICS/OT environments can be effectively managed.

Having an effective vulnerability management process in place also supports several Outcomes within the NCSC's Cyber Assessment Framework (CAF). A summary of the related Indicators of Good Practice (IGP) covered in this guidance is shown at the end of this article.

Meet 'Admin Corp'

Let's imagine we're following a fictional organisation who are responsible for managing the cyber security of a CNI processing plant.

Admin Corp runs a plant that produces Adminox, a highly volatile, refined form of administrative paperwork that is essential to every organisation in the country. It is created from volatile raw products using a continuous chemical process.

As an essential service, Admin Corp must comply with the UK NIS Regulation. This means that Admin Corp's assets needed to produce Adminox must be protected from cyber-attack. Also, because Admin Corp are regulated for safety by the UK Health and Safety Executive using OG86 , they must take steps to ensure the continued cyber security of the Adminox production process.

The Adminox processing plant has a fairly typical arrangement for this type of facility:

- **Process Control System (PCS) network**. This network hosts the main ICS/OT for the Adminox process. It comprises primarily of Programmable Logic Controllers (PLC)s that automatically operate the process, with some Human Machine Interfaces (HMI)s providing operators with localised viewing (as clients of the site Supervisory Control and Data Acquisition (SCADA) system, while others provide independent control of individual process areas. The network is an Internet Protocol (IP) based network compromising of managed Ethernet switches. The network is logically separated into Virtual Local Area Networks (VLAN)s to allow segregation of individual process areas.
- **Control Room**. This provides a centralised position for operators to control and monitor the plant using a SCADA system comprising of servers and workstations. The SCADA system operates in a dedicated VLAN.
- **Business Network**. This hosts IT infrastructure that is not involved in the production of Adminox; however, has connectivity to the control room and PCS networks to allow:
  - Consumption of process data by IT systems to support business operations.
  - Verified system updates to be passed from IT systems to the ICS/OT infrastructure.
- **Network firewalls**. These controls the data connection between the various ICS/OT VLANs, including between the control room and remote sites, in addition to between the ICS/OT and IT environments.

- **Safety Instrumented System (SIS) network**. This network is physically isolated from the control room and PCS networks, and ensures the plant reverts to a safe operating condition should a dangerous fault condition occur within the processing plant. It does, however, have a data-diode on the network allowing outbound event data to be sent to the SCADA system, but without any inbound communication paths that could be used as an ingress point for threats.

Vulnerability Identification

Controlling the Adminox production process on the PCS network is an EagleEye SCADA system communicating back to a centralised service.

Through their regular monitoring of the US Cyber Security Infrastructure Security Agencies ICS/OT notifications of vulnerabilities, via a dashboard project a new vulnerability, Log5k, was identified in the firmware of all LegAC PLC devices.

Vulnerability Prioritisation

The vulnerability is ingrained within the communication protocol used by LegAC PLCs over TCP port 3456 and as this is a required element of the system reducing the potential mitigation strategies. The exploit has two elements:

- Element 1 - A malicious packet using command code 4 can be used to switch the PLCs operating state to stop mode.
- Element 2 - A malicious packet using the command code 5 can be used to replace the ladder logic of the PLC with that crafted by the attacker.

The remediation process defined by the manufacturers is to update to the latest version of the firmware and the problem is fixed. Unfortunately, Admin Corp is faced with several problems that means that this situation is not easy to solve:

- The LegAC PLCs devices were installed 7 years ago, since then Admin Corp have changed the underlying hardware within LegAC PLCs and consequently the new firmware will not run on the legacy devices.
- The safety certification of the EagleEye SCADA system means that any update would need to be validated in an identical test environment for 6 months and all impacts related to the changes identified.
- Admin Corp already has a Network Traffic monitoring solution deployed monitoring the traffic to/from the Engineering Workstations

- Admin Corp does not currently have the funds available to replace the entire system.
- The risk appetite for Admin Corp is too low for them to accept the risk of allowing the vulnerability to exist unchecked.
- To ensure compliance with Health & Safety regulations the vulnerability must be resolved.

As such, the response to this vulnerability was prioritised as needing to be implemented 'now'.

The CVSS rating for this vulnerability was 7.2, at the same time a Common Vulnerability Enumeration (CVE) for another vulnerability impacting some Admin Corp systems, Eternal Green, was also released. The Common Vulnerability Scoring System (CVSS) for Eternal Green was 8.2. After discussion with the Engineering team responsible for the Adminox process it was realised that Log5K had the potential for much greater impact, with the capacity to halt production altogether. This greater impact meant that even though the CVSS score might be lower, the decision was taken to prioritise Log5k (highlighting that more than just the CVSS score should be taken into account, especially within ICS/OT environments).

Decisions to Make

Due to the immediate nature of the Log5K threat Admin Corp decided that they could not wait until the next scheduled downtime, which was not scheduled for another 2 months, they needed to provide a mitigation as soon as possible which meant implementing a solution whilst the process continued to run. Therefore, the options to reduce the ability to exploit the vulnerability were reviewed.

In reviewing its asset management knowledge base, Admin Corp realised that the update released by the vendor would need thorough testing and that the verification process required for their safety certification required months of validated testing within a controlled environment, months Admin Corp did not have.

Admin Corp investigated whether they could update all of the affected PLCs. Unfortunately the available funding was not enough to cover the cost of updating all the PLCs and the loss of revenue from halting the process to allow the upgrades was deemed unacceptable. This restricted the options further and so isolating all LegAC PLCs was considered. Unfortunately, the connectivity to other ICS/OT elements was necessary for the process to run and so this solution was deemed non-viable meaning Admin Corp would be forced to develop a bespoke solution.

Mitigation Implementation

Taking into account resources available and the modifications that could be allowed Admin Corp decided that the following two-fold solution be implemented:

- **Virtual Patch:** After assessing the operation of the system the engineers determine that the remote state switching is not necessary on the PCS network, if a change in state is required this can be done manually. Therefore, a virtual patch is applied on all firewalls with an interface to the ICS/OT environment, including between various ICS/OT VLANs, between the control room and remote sites, in addition to between the ICS/OT environment and the IT environments. The firewalls all with Deep Packet Inspection capabilities for the communication protocol, are configured to block all communications on TCP Port 3456 using command code 4 (and providing alerts back to the Industrial Intrusion Detection System monitoring solution).

- **Enhanced Monitoring and alerting & respond and recover:** To combat the threat Admin Corp developed new rules within their existing network logging and monitoring solution, configured to alert on instances of command 5 on TCP Port 3456. A response instruction was also produced, identifying the steps to be taken by an analyst to determine if this represented malicious activity, allowing for the reporting of such activity to the plant operations and engineering teams to progress the necessary response to prevent an unacceptable consequence from being realised.

Final Thoughts

Admin Corp also recognised that these solutions, whilst providing immediate protection, did not remove the residual risk that the vulnerability could be exploited if circumstances changed, or new exploits were developed.

While continuing to monitor sources for vulnerability and exploit notifications, additional steps were also taken to monitor for the triggering of either alert, with all such occurrences recorded in the relevant system history. This facilitated monthly periodic reviews of the threat to these systems allowing for further remedial action to be undertaken.

Additionally, the implementation of these vulnerabilities, and the applied mitigations, was recorded in the systems annual health reports and used to assess the justification for any further work and further revenue expenditure/investment.

CAF IGP Summary

This case study discusses measures that contribute to the following CAF IGPs:

- B4.d.A1 - You maintain a current understanding of the exposure of your essential function(s) to publicly known vulnerabilities.
- B4.d.A2 Announced vulnerabilities for all software packages, network and information systems used to support your essential function(s) are tracked, prioritised and mitigated (e.g. by patching) promptly.
- B4.d.PA3 - Some vulnerabilities that are not externally exposed have temporary mitigations for an extended period.
- B4.d.PA4 - You have temporary mitigations for unsupported systems and software while pursuing migration to supported technology.

In addition this case study supports the requirements within the HSE's OG86, Cyber Security for Industrial Automation and Control Systems (IACS) - notably Appendix 2, B4 System Security.

Statement of Support

This guidance has been produced with support from members of the Industrial Control System Community of Interest (ICS-COI) for publication via the Research Institute for Trustworthy Inter-connected Cyber-Physical Systems (RITICS), with support from the National Cyber Security Centre (NCSC). This guidance is not intended to replace formal NCSC guidance where already available, and care has been taken to reference such existing guidance where applicable.

This document is provided on an information basis only, ICS-COI members and NCSC have used all reasonable care in verifying the guidance contained within using the data sources available to it, they provide no warranty as to its accuracy or completeness. To the fullest extent permitted by law, the NCSC and the ICS-COI accept no liability whatsoever for any expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the report or arising from any person acting, refraining from acting, relying upon or otherwise using this document. You should make your own judgment as regards use of this document and seek independent professional advice on your particular circumstances.

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer or otherwise, does not constitute or imply its endorsement, recommendation or favour by the ICS-COI or NCSC. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.