tyco

security

exacqVision

Cybersecurity Overview

Whitepaper

Version 1.0
Date: 24-May-2018

Johnson Controls

Introduction

The Tyco security, Cyber Protection Product Security Program provides peace of mind to our customers with a holistic cyber mindset beginning at initial design concept, continues through product development, and is supported through deployment, including a rapid incident response to meet the comprehensive and evolving cybersecurity environments.

The Exacq Cybersecurity Overview Whitepaper is intended to provide cybersecurity guidance used in planning, deployment and maintenance periods.

As cybersecurity threats have become a risk impacting all connected devices, it is important to assure that cybersecurity is considered throughout the planning, deployment and maintenance phases associated with a product's functional operation.

This guide provides hardening guidance for configuration and maintenance, password strengthening and authentication recommendations, including the operating system's user accounts and services with their permissions and roles.

1 Introduction to Exacq

The Exacq video management solution, comprised of a video management system (VMS), video servers, and network video storage servers, is known for its ease of install and use, and low maintenance costs.

The powerful exacqVision VMS is available on factory-installed hybrid and IP servers, and works with a wide range of commercially available off-the-shelf servers. Its intuitive and powerful feature set make it an ideal choice for many security-conscious applications, including those in education, retail, healthcare, and finance. exacqVision allows customers to easily manage live and recorded video, from small stand-alone system to sprawling enterprise applications.

Compatible with thousands of IP camera models and dozens of access control, intrusion, and point-of-sale systems, exacqVision's integrations make it one of the most robust end-to-end security solutions in the industry.

2 Server (Desktop Platforms)

This section details manual remediation steps that provide greater security for exacqVision Server, when installed on desktop platforms including Windows 7 or newer, Ubuntu 10.04 or newer, S-Series, and M-Series.

1. Remediate Server Service

To remediate a desktop Linux or M-Series system, execute the following script with sudo and then reboot the system:

```
#!/bin/bash
/etc/init.d/edvrserver stop
adduser --system --group --shell /usr/bin/nologin edvrserver
usermod -G audio,dialout,cdrom edvrserver
chown -R edvrserver:edvrserver /mnt/edvr
sed -i 's/--start/--start -c edvrserver:edvrserver/' /etc/init.d/edvrserver
if grep -q poeinfo /proc/cpuinfo; then
    echo 'SUBSYSTEM=="misc", KERNEL=="i2c", ACTION=="add",\
GROUP="edvrserver", MODE="0660"' >> /etc/udev/rules.d/91-permissions.rules
    chown -R edvrserver:edvrserver /opt/exacq/server
else
    chown -R edvrserver:edvrserver /usr/local/exacq/server/
fi
```

To remediate an S-Series system, the administrator must disable the *edvrservice* from automatically starting. It should be manually started when performing a configuration, then stopped when re-configuration operations have been applied. The following steps explain how this can be accomplished:

1. Stop *edvrserver* service.
2. Disable */etc/init.d/edvrserver* from automatically starting at boot.
3. To configure, manually start *edvrserver* service, then manually stop service once configuration has successfully been applied.

On Windows systems, exacqVision Server always installs as *Local System*, which grants unlimited OS administrative privileges to the software. This could pose a security threat if the OS itself becomes compromised. This can be mitigated by configuring the exacqVision Server service to instead run as *Local Service*, which is considered more secure for a long-running Windows service that accepts incoming network connections. To make this change, follow these steps:

1. Stop the *exacqVision Server* service.
2. Right-click on *Service* and select *Properties*.
3. On the *Log On* tab, select *This Account* and enter “Local Service.”
4. Clear both password controls.
5. Click *Apply*.
6. The services control panel should now indicate *Local Service* for service.
7. In order to use LDAP and/or notification, and for the server to successfully log activity, grant full control permissions for regular users to the *data* and *logs* subfolders. If this step isn’t done, *LogPI* will fail to load and return “error -2.”
8. Start the service. Task Manager should show "core" process running as *Local Service*.

2. Change Default User Account Passwords

Unless a user has deliberately changed them, older servers will have a default username and password for the administrator and user accounts. We recommend changing both of these default passwords to prevent unauthorized access to exacqVision.

Starting with version 9.4 of exacqVision Server, the installer forces the user to change the default full admin password. However, systems that are upgraded from an older exacqVision version to version 9.4 will not force this password reset.

3. Enable Password Strengthening and Augmented Authentication Feature

This feature, introduced in exacqVision Server version 9.0, enables a more secure communication protocol between the client and server, by which the server can more tightly enforce authentication controls. Once a user upgrades both the client and the server to version 9.0 or newer, the client will feature a *Security* tab where this feature can be enabled.

Once the user has done this, machines running older versions of exacqVision Client will no longer be compatible with the server. This is the desired behavior because older Client versions allow the setting of weak passwords, whereas newer Client versions (9.0 or higher) force users to set strong passwords.

Passwords themselves will be stored using a salt and hash. This helps prevent a server from becoming compromised in the event someone gains access to the password file because passwords that are salted and hashed cannot be converted into cleartext. Passwords are then further strengthened with the Argon2 key extension algorithm, thereby making dictionary or brute-force attacks much more time-consuming for attackers.

4. Discontinue Using External Systems That Do Not Require Authentication

If you use the e-mail notification feature, ensure that you only use an SMTPS server that requires password authentication, and also requires SSL.

If you use the AD/LDAP integration feature, ensure that you only use an LDAP server that requires password authentication, and also requires SSL.

If you connect an intrusion panel or an access control system, ensure that you only connect to systems that require password authentication or some sort of secret key mechanism.

If you use the archiving feature, ensure that you only connect to SMB targets that require password authentication.

5. Unavailable Functionality as a Result of Hardening

The following functionality has been verified as unavailable when the above server hardening steps have been applied:

1. Windows Systems

1. Remote updates will fail with the error message "installer failed to launch." The server must be manually updated.
2. Server failover: The user must employ a third-party solution.
3. The exacqVision DHCP service cannot be used. The user must implement their own DHCP server on the camera network.
4. Time/Date Configuration: The user can change the time/date/time zone configuration, but not the network transfer protocol. The user must manually configure the NTP via Windows Control Panel.
5. Extended storage (iSCSI) support: The user must manually configure the iSCSI initiator.
6. Motherboard sensor monitoring (voltage, fan, temperature): No workaround is available.
7. Motherboard hardware watchdog support: The user will have to configure a Windows task with administrator privileges.

8. Storage hardware monitoring: The user must employ a third-party solution like *smartd* or rely upon RAID management software.
9. Drive self-test functionality: The user must manually partition, format, and mount disks.

2. Linux / M-Series Systems

1. Remote Updates: Remote updates will fail with the error message "installer failed to launch." The server must be manually updated.
2. Server failover: The user must employ a third-party solution.
3. Network Configuration Changes: Network configuration changes will be ignored. The user must manually configure the network outside of Exacq software.
4. The exacqVision DHCP service cannot be used. The user must implement their own DHCP server on the camera network.
5. On M-Series systems, IP auto-connect will be unavailable. The user must statically configure all PoE IP cameras.
6. Time/Date Configuration: Changes to the time, date, time zone, or NTP are ignored. The user must manually configure them outside of Exacq software.
7. Archiving support: The user must manually edit *fstab*.
8. Extended storage (iSCSI) support: The user must manually configure the iSCSI initiator and edit *fstab*.
9. Motherboard sensor monitoring (voltage, fan, temperature): No workaround is available.
10. Motherboard hardware watchdog support: The user will have to configure a *cron* script with administrator privileges.
11. Storage hardware monitoring: The user must employ a third-party solution like *smartd* or rely upon RAID management software.
12. Drive self-test functionality: The user must manually partition, format, and mount disks.

3 Web Service

This section details manual remediation steps that provide greater security for exacqVision Web Service, when installed on desktop platforms including Windows 7 or newer, Ubuntu 10.04 or newer, S-Series, and M-Series. Remediation of the Web Service is performed in the steps outlined below.

1. Enable TLS (HTTPS):

TLS connections require a user-specific certificate and must be manually configured to be enabled. Utilizing TLS in all web communication is highly recommended as it actively prevents reading and manipulation of communication between the client and the web service. TLS connections are provided in the web service through two mechanisms:

1. Let’s Encrypt/ACME: A free service to provide TLS certificates with minor restrictions (the web service must be hosted on port 80 and a domain name must be associated with the web service).
2. External: User-supplied certificates for TLS. These certificates are purchased from a certificate authority, such as VeriSign, DigiCert, or Network Solutions.

From the web service and end-user perspectives, there is no functional difference between the two types of configuration.

To configure TLS in the web service:

1. Log into the web service configuration by clicking the “Web Service Configuration” link on the web service landing page.
    - If this link is not displayed, the “Restrict to localhost” setting is enabled. Either access the web service directly from the machine or disable this setting.
2. Select Configuration -> HTTPS from the navigation menu.
3. Click the Configure button.

4. From the drop down, select the desired configuration type (Let’s Encrypt or External).
5. Supply the required information for the selected type and click Apply.
6. Restart the web service when prompted. The web service is now reachable via HTTPS.

2. Modify System Settings (Windows Only):

Reconfigure the exacqVision Web Service service to instead run as "Local Service." The Web Service always installs itself as Local System, which grants unlimited OS administrative privileges to the software. This may be construed as a security risk if the OS itself becomes compromised. The *LocalService* account is considered more appropriately secure for a long-running Windows Service that accepts incoming network connections. To do so:

1. Stop the exacqVision Web Service and exacqVision Web Server services.
2. Right-click on each service and select *Properties*.
3. On the *Log On* tab, select *This Account* and enter "Local Service".
4. Clear both password controls.
5. Click *Apply*.
6. Services control panel should indicate "Local Service" for service.
7. Start the services. Task Manager should show multiple *evws* processes and a *wfe* process running as *LOCAL SERVICE*.

3. Unavailable Functionality as a Result of Hardening:

Due to the nature of some of the remediation steps, the following functions become unavailable when these steps have been applied:

1. Updates (Windows Only): Attempting to update the web service through the service configuration will result in an error message of “An error occurred while installing the update.” The web service must be manually updated.
2. Restarting (Windows Only): Attempting to restart the web service through the service configuration will result in an error message of “There was an error

during restart.” The web service must be manually restarted using the Windows Services utility or through the provided Start Menu shortcuts.