tyco

security

exacqVision 19.03

Cybersecurity Overview

Whitepaper

Version 1.0
Date: 15-March-2019

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 NVR or S-Series Server Service for 9.8 or older

We recommend that you upgrade to 19.03 or newer, to maintain all software functionality while de-elevated. If you are unable to upgrade, please refer to previous revisions of this document for instructions, and a list of features that will become unavailable.

2. Remediate S-Series Server Service for 19.03 or newer

S-Series servers may be remediated identically to NVR servers. No additional steps are required.

3. Remediate NVR Server Service for 19.03 or newer

To remediate a desktop Linux or M-Series system:

- **You must first delete any existing archive targets, and plan to create entirely new archive targets. Otherwise, archive targets will be unable to connect after transitioning to de-elevation or vice versa.**
    - **Note – this includes cloud archiving targets. In such cases, you will need to first ensure you know the credentials for your exacq Cloud Drive account, so that once you either de-elevate or re-elevate, you will be able to re-create the cloud archiving target with correct credentials.**
- Execute the following command. When so prompted, answer “yes” to de-elevate, or “no” to re-elevate:
    - `sudo dpkg-reconfigure –p low edvrserver`
- The service will automatically restart itself appropriately.
- You can then execute the “ps agux” command to verify that the processes named “core” and “exacqd” are both running as the “edvrserver” user, instead of the “root” user.
- The NVR will still be able to record and search, and a local client running as non-administrative OS user will be able to search, because 755 permissions (service has full access, all other users have read-only access) are automatically applied recursively to all relevant local recording drives.
- Now you may create new SMB, NFS, and/or cloud archive targets as necessary.

To remediate a Windows system:

- Unlike with Linux, you may continue using existing SMB or NFS archive targets after transitioning to de-elevation or vice versa. This is due to fundamental differences between the Windows security model and the Linux security model.
- **However, this is not true for cloud archiving targets. In such cases, you will need to first ensure you know the credentials for your exacq Cloud Drive account, so that once you either de-elevate or re-elevate, you will be able to re-create the cloud archiving target with correct credentials.**
- **Then, you must execute the following commands as an OS-administrative user for each enabled recording drive (using d:\ as an example):**
    - `icacls d:\ /grant “Network Service:f” /t`

    - `icacls d:\ /grant “Users:rx” /t`
- Stop service. Add the following line to PluginList.ini to de-elevate, or remove it to re-elevate:
    - `deelevate=true`
- Start service once again.
- You can then use Task Manager to confirm that the processes named “core” and “exacqd” are both running as the Network Service user, instead of the “SYSTEM” user.
- The NVR will still be able to record and search because you have manually granted permission for the Network Service user to be able to read, write, and delete files on all relevant local recording drives.
- Local clients running as non-administrative OS users will be able to search because you have manually granted read and execute permissions for all valid OS users to all relevant local recording drives.
- Now you may create new SMB, NFS, and/or cloud archive targets as necessary.

4. Change Default Operating System Passwords

Unless a user has deliberately changed them, older servers will have a default username and password for each operating system user account. We recommend changing all operating system passwords to prevent unauthorized access via local or remote desktop or secure shell sessions.

5. Change Default exacqVision User Account Passwords

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

Starting with version 9.4 of exacqVision Server, the installer forces the user to change the default full admin password when installing for the first time. However, upgrading an existing system will not force this password reset.

6. 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 for setting weak passwords, whereas newer Client versions (9.0 or higher) force users to set strong passwords.

When this feature is enabled, actual passwords will not be stored. Instead, a secure identifier will be generated using a strong algorithm that combines a salt and hash with the Argon2 key extension algorithm and additional encryption. This secure identifier is what will be stored instead. This helps to prevent a server from becoming compromised if someone gains access to the password file, because passwords that are salted and hashed cannot be converted into cleartext. Further, the use of a key extension algorithm makes dictionary or brute-force attacks much more time-consuming for attackers.

7. 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 as well as SSL.

If you use the AD/LDAP integration feature, ensure that you only use an LDAPS server that requires password authentication for binding, as well as 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 connect to IP cameras or encoders, ensure that you only connect to devices that require password authentication as well as SSL.

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

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.