MARCH NETWORKS PRODUCT HARDENING GUIDE

The March Networks Product Hardening Guide provides recommendations for Technicians and System Administrators installing March Networks products within a customer's network to help ensure security. The security level should be selected based on the customer's internal security policies and/or security audit.

The products covered under this hardening guide:	
X-Series Recorders	version: 6.1.x
8000/9000/RideSafe Series Recorders	version: 5.20.x
6700 Series NVRs	version: 2.5.x
Command Recording Software	version: 2.10.x
Command Enterprise	version: 2.12.x
EDGE OS Devices	version: 1.10.X - 1.11.x
EDGE OS II Devices	version: 2.4.x - 2.5.x
ME/SE Series Cameras	version: 1.0.x - 1.1x

Security Levels Explained

Level 1 – No Protection (default)	Level 2 – Moderate Protection	Level 3 – High Protection
Settings found on product when originally purchased from manufacturer.	Settings recommended to provide a moderate level of security while still enabling network/remote configurations by the systems administrator.	Settings recommended for the highest level of security. Please read the Impact descriptions carefully before applying.

IMPORTANT LINKS:

March Networks Partner Portal: https://partners.marchnetworks.com (username/password required)

March Networks Security Updates and Advisories: https://www.marchnetworks.com/support-downloads/technical-support/security-updates-and-advisories/

X-SERIES RECORDERS

Item ID	Item Description	Possible Vulnerability	How-To	Security Level 1 (default)	Security Level 2	Security Level 3	Security Level 3 Impact	Configured using...	Reference
X-Series Install Defaults	During a recorder installation, if you are not working with a brand new recorder, start by resetting the device to manufacturer's default settings.	If a device is not brand new out of the box, a previous configuration may expose vulnerabilities. Start with a known default configuration before configuring the recorder during installation.	Using Command Config, log on to the X-Series recorder. On the main page, under General Settings, click System. Under Operations, click Reset.	All new products are shipped with manufacturer's default settings.	Reset the configuration to defaults before configuring a device not recently purchased from the manufacturer.	Reset the configuration to defaults before configuring a device not recently purchased from the manufacturer.	When applying manufacturer settings, all current settings on the device will be lost. All cameras currently connected will disconnect. IP cameras/ encoders will have to be re-added to the device.	Command Config	X-Series R6 Hybrid NVR Configuration Guide – Chapter 7 Configuring System Settings
X-Series Communication Ports	Use secure HTTPS communication to access the device by way of an Internet Browser, Command Config or Commnand Client.	Communication over the default HTTP port could be vulnerable to "sniffer attacks". When configuring sensitive information on the device, such as user accounts and passwords, access the recorder using HTTPS. Note the default HTTPS port on X-Series is 44300	Using Command Client, Log on directly to the recorder. Within the System tree, right-click on the recorder icon and select Open. Click Edit Addresses. Change the default ports of 8000 or 44300 as required.	Communication over HTTP and HTTPS is enabled by default on X-Series recorders.	Although you may not turn off the HTTP access, you are able to change the port to something other than 8000.	Choose your own port for HTTPS communication.	The customized HTTPS port must be "open" between the recorder and your computer in order to configure it.	Command Client	Command Enterprise and Client User Guide – Chapter 6 Managing Recording Devices
X-Series Admin Password	Create a strong password for the default admin account. March Networks X-Series allows you to create strong passwords, as there are no restrictions on the number of characters used other than the following character: You may not use "$" in the password field.	Never leave the default password blank. Apply a strong password to the Admin account following the customer's password creation policies.	Using Command Config, log on to the X-Series recorder. On the main page, under User Management, click Users. Select the Admin user and click Edit Security Settings. Click Password Substitution and enter a strong password. Click Ok.	March Networks X-Series recorders require an Admin password be created using Command Config, on the first log on attempt.	Set the same strong password for all X-Series recorders Admin accounts following the company's password creation policies.	Set strong individual passwords for the Admin account on each X-Series recorder on the network. Do so following the company's password creation policies. Add an identification certificate to enhance security.	With individual passwords per X-Series recorders, good password management becomes critical. A USB token or smartcard is required to add an identification certificate.	Command Config	X-Series R6 Hybrid NVR Configuration Guide – Chapter 4 Managing User Profiles

Item ID	Item Description	Possible Vulnerability	How-To	Security Level 1 (default)	Security Level 2	Security Level 3	Security Level 3 Impact	Configured using...	Reference
X-Series Software Updates	Keep the X-Series recorder at the most up-to-date software version. Latest software is available for download from the March Networks Partner Portal. Subscribe to March Networks Security Updates and Advisories email alerts online to stay up-to-date.	The latest X-Series software provides not only new features and bug fixes, but ensures any known vulnerabilities are addressed, preventing exploitations.	Download the latest X-Series software from the Partner Portal. Place the file on the computer where Command Config software has been installed. Log on to the recorder using Command Config. On the Main page, select System. Select Upgrade from the Software area. Locate the .upgx file recently downloaded and follow the prompts.	X-Series recorders are shipped to customers with a minimum ship level software. This software version may be several versions behind the latest posted software found on the Partner Portal.	Update X-Series software to the latest release found on the Partner Portal. Note: If the recorder is managed by a CES, do not upgrade the recorder's software beyond that of the CES software version.	Load latest X-Series update file on Command Enterprise and update all recorders automatically using CES' Mass Management feature.	Command Enterprise is required for automation of recorder software application.	Manually using upgrade file with Command Config or using Command Enterprise Mass Management feature.	X-Series R6 Hybrid NVR Configuration Guide – Chapter 7 Configuring System Settings
X-Series User Accounts, X-Series Managed by CES	When an X-Series recorder is being managed by a CES, user accounts requiring access to the recorder should be created on the CES and authenticated by the CES.	Creating local accounts on the X-Series software when the recorder is being managed by a CES creates additional means of authentication and possible exploitation. Local accounts should be disabled.	Using Command Config, log on to the X-Series recorder. On the Command Config main page, under User Management, click Users. Delete all local user accounts. Click Ok. Alternatively, under System, System Configuration, select Disable standard local users from the Users area.	By default, only the admin account is created on an X-Series recorder.	Delete each local user account other than the admin account. Alternatively, use the Disable standard local users feature to disable all local users (you may also disable local LDAP users).	Use the Disable standard local users feature as well as the Disable local user "admin" feature to ensure no local user accounts can be used to authenticate locally to the recorder.	All client authentications must be done through the Command Enterprise Server. Access to the CES is therefore a requirement for all Clients.	Command Config	X-Series R6 Hybrid NVR Configuration Guide – Chapter 7 Configuring System Settings
X-Series User Accounts, Non-CES Managed Environment	When creating user accounts, use strong passwords as per customer's password creation policy. Make use of the Password Policy features of the recorder. Enable User profile security settings (password substitution, expiration date, max sessions, change password every, etc.) for each user. Consider using secondary means of validation, such as certificate, or you may use LDAP.	When Password Policy features are not used, a user may create a very weak password. Without the User profile Security settings enabled, local user passwords are created and never changed or updated, exposing potential security issues.	Using Command Config, log on to the X-Series recorder. On the Command Config main page, click System. Enable the appropriate Password Policy features, within the Users area, as per customer password creation policies. On the Command Config main page, under User Management, click Users. Select a user and click Edit Security Settings. Enable the specific Security settings as required by customer policies. Click Ok. Click Save Changes.	By default, Password policy features and user profile security settings are disabled for local users	For each local user profile, enable the following according to the customer's policies: Enable Minimum Password length and require a password to contain at least one upper case, number or special character. Change Password Every X days. Set the Concurrent Max Sessions to 1. Set a Profile Expiration Date. Use a secondary means of authentication like a smartcard.	Switch from local users to LDAP users in order to make use of Active Directory password policies. This also ensures your user credentials are stored in a single location.	LDAP must be in use on the network.	Command Config	X-Series R6 Hybrid NVR Configuration Guide – Chapter 4 Managing User Profiles

Item ID	Item Description	Possible Vulnerability	How-To	Security Level 1 (default)	Security Level 2	Security Level 3	Security Level 3 Impact	Configured using...	Reference
X-Series MaxUser Connection	Set the Max Simultaneously Connected Users setting to the number of actual users accessing the system (including administrator) to prevent access attempts by non-authorized users. When all authorized users are connected, no other log on attempts are permitted.	By leaving the default setting in place, unauthorized users may access the recorder's Log on page and try to gain access to the system.	Using Command Config, log on to the X-Series recorder. On the main page, under General Settings, click System. Under Users, set the Max Simultaneously Connected Users count to the number of users permitted to log on. Click Save Changes.	By default, the Max Simultaneously Connected Users is set to 32 users/clients.	Set the Max Simultaneously Connected Users setting to the number of actual users accessing the system.	Set the Max Simultaneously Connected Users setting to the number of actual users accessing the system.	The Max Simultaneously Connected Users setting will need to be updated for all new client users added to the system.	Command Config	X-Series R6 Hybrid NVR Configuration Guide – Chapter 7 Configuring System Settings
X-Series Encrypted Sockets	If using the legacy software application SiteManager with the X-Series recorders, enable the encrypted sockets feature to provide additional security by encrypting the traffic data between the recorder and SiteManager.	Given SiteManager connects with X-Series recorders over an unsecured port, the data between it and the recorder is susceptible to be viewed.	Using Command Config, log on to the X-Series recorder. On the main page, under General Settings, click System. Under Network Interfaces, select the 0/0 Network interface and select Use Encrypted Sockets. Click OK and Save Changes.	By default, the Use Encrypted Sockets feature is disabled.	Enable Use Encrypted Sockets if SiteManager must be used with an X-Series recorder.	Enable Use Encrypted Sockets if SiteManager must be used with an X-Series recorder.	None	Command Config	X-Series R6 Hybrid NVR Configuration Guide – Chapter 7 Configuring System Settings
X-Series NAT Traversal Communication	NAT Traversal allows access to an X-Series recorder and its camera streams without opening inbound firewall ports on the recorder's network and does not require the addition of specific routing rules. Note: if NAT Traversal is enabled, but ports remain open on the firewall, Clients will default to port based communication if the recorder responds on such ports.	Option 1 – If the recorder is not remote to your network, and there are no remote Clients requiring access to the recorder, you may disable the NAT Traversal feature. Option 2 – If you prefer to use NAT Traversal to allow access to a remote Client or remote recorder, especially to keep the recorder up-to-date with new software versions and patches, it is recommended to enable NAT Traversal communication. This type of connection uses Secure DTLS protocol for authentication and encryption between the Client and X-Series recorder.	Using Command Config, log on to the X-Series recorder. On the main page, under General Settings, click System. Select Network Interfaces. Enable or disable the Use NAT Traversal feature as required. The feature is enabled by default on all recorders. Click Save Changes.	On a new recorder NAT Traversal is enabled by default. Note: Once enabled NAT Traversal communication will not be used by Clients unless enabled on the Command Enterprise, where the recorder in question must be registered, and the user is provided the NAT Traversal right within their profile.	Option 1 – If NAT Traversal is not required, it can be disabled. Option 2 – Make use of NAT Traversal.	Option 1 – If NAT Traversal is not required, it can be disabled. Option 2 – Make use of NAT Traversal.	When Command Client uses NAT Traversal communication with an X-Series recorder, the Client loses the ability of accessing the web page (camera settings) of any IP cameras or encoders connected to that recorder's camera network interface.	Command Config	X-Series R6 Hybrid NVR Configuration Guide – Chapter 7 Configuring System Settings

Item ID	Item Description	Possible Vulnerability	How-To	Security Level 1 (default)	Security Level 2	Security Level 3	Security Level 3 Impact	Configured using...	Reference
X-Series Identification Certificates	You can enhance the security of an X-Series recorder by adding identification certificates. Identification certificates are included in specific USB tokens or smartcards. Certificates can be linked to the recorder's connection (via Command Config, Command Client) or to specific recorder features. This adds an extra level of security at the recorder and between it and the client user.	None. Adds extra level of security.	Insert the USB token or smartcard, containing the identification certificate, on to the client computer. Using Command Config, from the main page, select Certificates from the User Management area. Click Import. Select a Certificate in the list and click Ok. Click Save Changes.	Identification Certificate for End-to-End Encryption is enabled by default.	Enable identification certificates by obtaining (importing) one from USB token/ smartcard and saving it on the recorder and on the client.	Enable identification certificates by obtaining (importing) one from USB token/ smartcard and saving it on the recorder and on the client. Assign certificates to specific features such as: -Archive Encryption. -End to End Encryption. -Playback Rights. -Export Rights. -Setup Rights	A USB token or smartcard is required. Cannot be used with LDAP/Active Directory users. Enabling Encryption on the recorder may impact its performance. Please review the recorder's software release notes for more details.	Command Config	X-Series R6 Hybrid NVR Configuration Guide – Chapter 6 Configuring Identification Certificates
X-Series TimeSync NTP	Use Command Config to set the recorder's time synchronization to an NTP server.	By leaving the time sync to the default "manual", the time of a recorder may drift, which affects log files and audits trails and makes it difficult to track attacks.	Using Command Config, log on to the X-Series recorder. On the main page, click System. Select System Time and click NTP. Enter the IP address or URL of the NTP time server within the address field. Click OK and then click Save Changes.	System Time is manually set.	System Time is changed to use customer's NTP server or a server on the internet.	System Time is changed to use customer's NTP server or a server on the internet.	NTP server must be in use on customer's network. Alternatively you may use an external (internet based) NTP server.	Command Config	X-Series R6 Hybrid NVR Configuration Guide – Chapter 7 Configuring System Settings
X-Series USB Ports	Visually inspect to ensure no USB devices have been left connected to the recorder's USB ports and that the WiFi LED is off.	USB devices such as WiFi dongles and/ or flash drives can present a potential security threat when left connected (and enabled) to a recorder. These may allow an unauthorized user to gain access to the recorder over WiFi or access media on a forgotten USB flash drive.	Visually inspect the front and rear of your recorders for any left over USB devices. Ensure the WiFi LED is off by pushing the WiFi button on the front panel.	Remove USB flash drives after transferring any media from recorder. Turn off the integrated WiFi dongle after connecting to the recorder using the GURU Smartphone application.	Remove USB flash drives after transferring any media from recorder. Turn off the integrated WiFi dongle after connecting to the recorder using the GURU Smartphone application.	Remove USB flash drives after transferring any media from recorder. Turn off the integrated WiFi dongle after connecting to the recorder using the GURU Smartphone application.	None	Physical Inspection of the recorder's front and rear USB ports as well as the integrated WiFi dongle.	X12 Series Hybrid NVR - Installation Guide
X-Series and Edge Devices (IP Cameras and Encoders)	When adding Edge devices to an X-Series recorder, make use of the isolated camera network interface (0/1 Network) on the recorder.	Edge devices left at their default settings (non-hardened) are vulnerable. As added protection, IP cameras cannot be "reached" or exploited from the customer's main network while they are connected to a recorder's camera network interface.	Create an isolated (from the customer's main network) camera network originating from the recorder's camera network interface. A simple multi-port PoE switch, which interfaces between that interface and all Edge devices, is all it takes.	Connect all Edge devices to the recorder's camera network interface (0/1 Camera)	Connect all Edge devices to the recorder's camera network interface (0/1 Camera)	Connect all Edge devices to the recorder's camera network interface (0/1 Camera)	Although March Networks branded Edge devices can be upgraded while connected to the camera network interface, many 3rd party cameras cannot. When using the recorder over NAT Traversal, you may not reach its connected IP device's settings page.	Physically connect the cameras to the interface. Then, configure the 0/1 Camera Network Interface using Command Config.	X-Series R6 Hybrid NVR Configuration Guide – Chapter 7 Configuring System Settings

Item ID	Item Description	Possible Vulnerability	How-To	Security Level 1 (default)	Security Level 2	Security Level 3	Security Level 3 Impact	Configured using...	Reference
8000, 9000 AND RIDESAFE SERIES RECORDERS									
Recorder Install Defaults	During a recorder installation, if you are not working with a brand new recorder, start by resetting the device to manufacturer's default settings.	If a device is not brand new out of the box, a previous configuration may expose vulner-abilities. Start with a known default configuration before configuring the product during installation.	Using Admin Console's Task Type Device Update, apply the Default Config patch found on the Partner Portal.	All new products are shipped with manufacturer's default settings.	Apply default config patch before configuring a device not recently purchased from the manufacturer.	Apply default config patch before configuring a device not recently purchased from the manufacturer.	When applying manufacturer settings, all current settings on device will be lost. All cameras currently connected will disconnect. IP cameras will have to be re-registered.	Admin Console	Administrator Console User Manual – Chapter 18 Upgrading Recorder Software
Recorder Communication Ports	Configure communication ports used by Administrator Console, Command Enterprise and the recorder's web interface.	NVRs have two TCP/IP ports enabled by default; primary port 80 and secondary port 2804. With port 80 opened, the recorder will respond to Admin Console requests when contacted using only its IP address. Do not use port 80 for higher security. When in a managed environment, recorder uses default port 8080 and 443 for Command Client and CES communication respectively.	Using an SSH software, connect to the recorder on port 22. Log on to the Provisioning Interface. Type Setports to make configuration changes to the primary or secondary communication ports of the NVR. Use the Setagentports command to make configuration changes to the Agent (Command Client communication) ports	On a new NVR, setports command is configured with: Port 1 = 80, Port 2 = 2804. The Command Client and Enterprise (CES) communication Agent ports are set to 8080 and 443 respectively.	Change primary port 80 to 2804, disable secondary port. Leave Command Client and CES ports at default.	Choose your own port number in place of 2804. Keep the secondary port disabled. Choose your own ports for Command Client and CES communications. When working with remote recorders, use NAT Traversal communication which does not require inbound firewall ports to be opened at the recorder's location.	With higher security levels, user must add recorders to Admin Console or view their web page using :2804 (or whichever port is configured) after the IP address in order to obtain communication. It is best to make changes to Command Client and CES ports before the NVR is registered to CES.	Putty – while accessing the Provisioning Interface. May also use Command Client interface (connecting directly to recorder) to change the Agent ports	Provisioning Interface Technical Instructions – setports command. Command Enterprise and Client Installation Guide – Chapter 2 Requirements and Setup for Command Enterprise
Recorder 802.1x-Based Authentication	IEEE 802.1X allows authentication of recorders, by an authentication server, before they can access the network. It also requires a network switch, with 802.1x port based authentication enabled, at the recorder's location.	None - Adds extra level of security. This prevents unauthenticated devices from accessing the network.	Using Admin Console's Task Type Device Configuration, under the General Tab, enable IEEE 802.1x	IEEE 802.1x is disabled by default	If the recorder will be connected to a network switch with port based authentication enabled, you may enable the recorder's 802.1x feature and select the appropriate EAP type that matches the authentication server requirements. EAP-PEAP (MSCHAPv2) would be an appropriate type.	If the recorder will be connected to a network switch with port based authentication enabled, you may enable the recorder's 802.1x feature and select the appropriate EAP type that matches the authentication server requirements. EAP-TLS would be a better choice at this level.	None- A Client certificate and Private Key must be provided to the recorder when using EAP-TLS.	Admin Console	Administrator Console user manual - Chapter 6 Specifying General Recorder Options

Item ID	Item Description	Possible Vulnerability	How-To	Security Level 1 (default)	Security Level 2	Security Level 3	Security Level 3 Impact	Configured using...	Reference
Recorder NAT Traversal Communication	NAT Traversal allows Client access to recorders and their camera streams without opening inbound firewall ports on the recorder's network and does not require the addition of specific routing rules. Note: if NAT Traversal is enabled but ports remain open on the firewall, Clients will default to port based communication if the recorder responds on such ports.	Option 1 – If the recorder is not remote to the network and there are no remote Clients requiring access to the recorder, you may disable the NAT Traversal feature. Option 2 – If you prefer to use NAT Traversal to allow access to a remote Client or remote recording device, especially to keep this device up-to-date with new software versions and patches, it is recommended to enable NAT Traversal communication. This type of connection uses Secure DTLS protocol for authentication and encryption between the Client and March Networks supported recording devices.	If local to the recorder, using SSH software, connect to the recorder on port 22 and log on to the Provisioning Interface. If remote to the recorder and using NAT Traversal communication, use Admin Console to initiate the SSH session over that type of connection. Type Setnat to make the appropriate configuration changes to the NAT Traversal mode of the recorder. Note that you must select Mode 3 to avoid disabling your provisioning access.	On a new NVR, NAT Traversal is set to Client & Provisioning Access mode by default. Note: Tunnelling to the web interface of an IP device connected to an NVR, using Admin Console, is not permitted using NAT Traversal communication. As well, this type of connection will not be used by Clients unless enabled on the Command Enterprise, where the recorder must be registered and the user is provided the NAT Traversal right within their profile.	Option 1 – If NAT Traversal is not required, it can be disabled using the Setnat provisioning interface command. Option 2 – Use NAT Traversal in Client & Provisioning Access mode.	Option 1 – If NAT Traversal is not required, it can be disabled using the Setnat provisioning interface command. Option 2a – Use NAT Traversal in Client Access only mode. (this disables remote provisioning access) Option 2b – Leave NAT Traversal in Client & Provisioning Access mode but do not assign the Remote Provisioning right to any user's profile within the CES and/or do not provide any Client's IP address within the Enterprise Console's NAT Traversal tab.	Remotely accessing the recorder's provisioning interface using Admin Console is not authorized when NAT Traversal Client Access mode is selected on the recorder or when the Remote Provisioning right has not been assigned to a user's profile within CES and the Client IP address was not entered within the CES' Enterprise Console NAT Traversal tab.	Putty – while accessing the Provisioning Interface locally. Admin Console – in order to access the same interface remotely.	Provisioning Interface Technical Instructions – setnat command Admin Console User Manual – Chapter 21 Troubleshooting the Network Connection and Rebooting Recorders
Recorder Software Updates	Keep the recorder at the most up-to-date software version. Latest software is available for download from the March Networks Partner Portal. Subscribe to March Networks Security Updates and Advisories email alerts online to stay up-to-date.	The latest recorder software provides not only new features and bug fixes, but ensures any known vulnerabilities are addressed, preventing exploitations.	Use the Admin Console's Task Type Device Update to send a UPG file to the recorder. You may also use Command Enterprise to automatically update all of your recorders' software with use of schedules and bandwidth limitation.	Recorders are always shipped to customers with a default minimum ship level. As of the fall of 2018, the min. ship version is 5.8.1 SP2	Update recorders to the latest release found on the Partner Portal using Admin Console or Command Enterprise software	Load latest recorder update file on Command Enterprise and update all NVRs automatically. Implement Default Firmware to Install on Device Connection feature within CES' Mass Management.	Command Enterprise required for automation of software/firmware application.	Administrator Console and Command Enterprise	Administrator Console User Manual – Chapter 18 Upgrading Recorder Software
Recorder Admin Password	Create a strong password for the default SSH admin account. There are no restrictions on the number or type of characters to use when creating a strong password for this account.	All recorders manufactured or repaired after January 1, 2020 will be shipped with a unique password set to be the recorder's serial number. Recorders shipped before that date had the default SSH Admin account password set to: admin Update this initial password for the security of the system.	Using an SSH software, connect to the recorder on port 22. Log on to the Provisioning Interface. Type Setpass to change the default Admin account SSH password to a strong password.	All recorders manufactured or repaired after January 1, 2020 will be shipped with a unique password set to be the recorder's serial number. Recorders shipped before that date had the default SSH Admin account password set to: admin	Change the SSH Admin account password on all recorders to use the same strong password following the customer's password creation policies.	Change the SSH Admin account password on all recorders to their own individual strong password following customer's password creation policies.	With individual SSH Admin account password per recorder, good password management becomes critical.	Putty (SSH software) – while accessing the Provisioning Interface	Provisioning Interface Technical Instructions – Setpass command

Item ID	Item Description	Possible Vulnerability	How-To	Security Level 1 (default)	Security Level 2	Security Level 3	Security Level 3 Impact	Configured using...	Reference
Recorder SSH Disable	Remote access to the Provisioning Interface is not possible without SSH enabled. Disabling it provides the highest level of security.	Disable SSH access to the recorder from the Provisioning Interface to prevent any remote/ over the network connection to the Provisioning Interface and access to its commands.	Using an SSH software, connect to the recorder on port 22. Log on to the Provisioning Interface. Type Setssh to enable/ disable the SSH access to the recorder.	SSH is enabled by default.	SSH should remain enabled to allow System Administrator remote access to Provisioning Interface commands for health and maintenance purposes.	SSH is disabled.	With SSH disabled, there is no remote access to the Provisioning Interface. A technician must be dispatched to the site for certain tasks. Technician will be required to use an Ethernet to USB adapter to access Provisioning Interface locally when SSH is disabled.	Putty (SSH software) – while accessing the Provisioning Interface	Provisioning Interface Technical Instructions – Setpass command
Recorder Client Passwords, Non-CES Managed Environment	In a non-managed environment, Secure the following client's (Admin Console or Command Client) access to the recorders using Setsecure Provisioning Interface command.	By default, client software may access a recorder without any password. Enable Setsecure to provide local software authentication. There are no restrictions to the number of characters to use when creating a password. Accepted characters are: '0123456789–=~!@#$%^&*() +[]\{|;':",./<>?abcd efghijklmnopqrstuvwxyz ABCDEFGHIJKLM NOPQRSTUVWXYZ	Using an SSH software, connect to the recorder on port 22. Log on to the Provisioning Interface. Type Setsecure to enable/disable the local authentication of the admin and viewer accounts.	Setsecure is disabled.	Enable Setsecure. Provide same admin and viewer passwords for all NVRs following the customer's password creation policies.	Enable Setsecure. Provide individual admin and viewer passwords for each NVR following the customer's password creation policies.	With individual passwords per recorder, good password management becomes critical.	Putty (SSH software) – while accessing the Provisioning Interface	Provisioning Interface Technical Instructions – Setssh command
Recorder TimeSync NTP	Use Administrator Console to set the time synchronization to NTP server.	By leaving the time sync to the default "manual", the time of a recorder may drift, which affects log files and audits trails and makes it difficult to track attacks.	Using Admin Console's Task Type Device Configuration, click General Tab. Using the Select Time Sync method, select NTP. Enter the IP or URL of the NTP server and click Apply Settings.	Time Synchronization is set to manual.	Time Synchronization is changed to use customer's NTP server or may use Command Enterprise Service time sync function	Time Synchronization is changed to use customer's NTP server or may use Command Enterprise Service time sync function	NTP server must be in use on customer's network. Alternatively you may use an external (internet based) NTP server or Command Enterprise Server	Administrator Console	Provisioning Interface Technical Instructions – Setsecure command
Recorder SNMP Disable	Simple Network Management Protocol is an Internet Standard protocol used to collect information about managed devices on IP networks.	Given that the recorder's implementation of SNMP is version 1 and it does not use Traps, it is best to leave it disabled.	Using an SSH software, connect to the recorder on port 22. Log on to the Provisioning Interface. Type Setsnmp to enable/ disable the feature.	SNMP is disabled by default.	SNMP remains disabled.	SNMP remains disabled.	None	Putty (SSH software) – while accessing the Provisioning Interface	Provisioning Interface Technical Instructions – Setsnmp command

Item ID	Item Description	Possible Vulnerability	How-To	Security Level 1 (default)	Security Level 2	Security Level 3	Security Level 3 Impact	Configured using...	Reference
Recorder USB Ports	Visually inspect to ensure no USB devices have been left connected to the recorder's USB ports.	USB devices such as WiFi dongles and/ or flash drives can present a potential security threat when left connected to a recorder. These may allow an unauthorized user to gain access to the recorder over WiFi or access media on a forgotten USB flash drive.	Visually inspect the front and rear of your recorders for any left over USB devices.	Remove USB flash drives after transferring any media from recorder. Remove USB WiFi dongles after connecting to recorder using GURU application.	Remove USB flash drives after transferring any media from recorder. Remove USB WiFi dongles after connecting to recorder using GURU application.	Remove USB flash drives after transferring any media from recorder. Remove USB WiFi dongles after connecting to recorder using GURU application.	None	Physical Inspection of recorder's front and rear USB ports	See specific recorder series Installation Guide to locate USB ports.
Recorder and Edge Devices (IP Cameras and Encoders)	When adding Edge devices to a recorder, make use of the isolated camera network interface on the recorder.	Edge devices left at their default settings (non-hardened) are vulnerable. As added protection, IP cameras cannot be "reached" or exploited from the customer's main network while they are connected to a recorder's camera network interface.	Create an isolated (from the main network) camera network originating from the recorder's camera network interface. A simple multi-port PoE switch, which interfaces between that interface and all Edge devices, is all it takes.	Connect all Edge devices to the recorder's camera network interface.	Connect all Edge devices to the recorder's camera network interface.	Connect all Edge devices to the recorder's camera network interface.	Although March Networks branded Edge devices can be upgraded while connected to the camera network interface, most 3rd party cameras cannot.	Physically connect the cameras to the interface. Then, configure the 0/1 Camera interface using Admin Console.	Administrator Console User Manual – Chapter 4 Device Installation Tasks
Recorder WiFi Network Interface	When working with RideSafe Mobile recorders with direct connection to a WiFi antenna module, make use of WPA which is the most secured WiFi security protocol on the recorder	When using outdated protocols such as WEP, the recorder and its communication over WiFi to Command Enterprise are vulnerable. Use the more secure WPA-Enterprise protocol (WPA-EAP with RADIUS auth. server)	Refer to the Provisioning Interface Technical Instructions – Setip and ScanWiFi commands	RideSafe recorders connected to a WiFi antenna module do not have any WiFi protocols enabled. WiFi is off by default.	Enable WPA (PSK or EAP) to authenticate with existing WiFi equipment at customer site. Use strong password following the customer's password creation policies.	Enable WPA–EAP and make use of Radius auth. Server at customer site. Use strong password following the customer's password creation policies.	May require to upgrade customer WiFi equipment to make use of WPA–EAP protocol.	Putty (SSH software) – while accessing the Provisioning Interface	Refer to the Provisioning Interface Technical Instructions – Setip and ScanWiFi commands
6700 SERIES NVRS									
6700 Install Defaults	During a recorder installation, if you are not working with a brand new recorder, start by resetting the device to manufacturer's default settings.	If a device is not brand new out of the box, a previous configuration may expose vulner-abilities. Start with a known default configuration before configuring the product during installation.	In a web browser, enter the following: http://<recorder's IP address>/setup. Log on to the recorder. On the Command Config main page, under System, click Settings, then click Factory Defaults.	All new products are shipped with manufacturer's default settings.	Apply manufacturer's default settings before configuring a device not recently purchased from the manufacturer.	Apply manufacturer's default settings before configuring a device not recently purchased from the manufacturer.	When applying manufacturer settings, all current settings on device will be lost.	Command Config	6700 Series Hybrid NVR Configuration Guide – Chapter 7 Configuring System Settings

Item ID	Item Description	Possible Vulnerability	How-To	Security Level 1 (default)	Security Level 2	Security Level 3	Security Level 3 Impact	Configured using...	Reference
6700 Software Updates	Keep the recorder at the most up-to-date software version. Latest software is available for download from the March Networks Partner Portal. Subscribe to March Networks Security Updates and Advisories email alerts online to stay up-to-date.	The latest 6700 recorder software provides not only new features and bug fixes but ensures any known vulnerabilities are addressed preventing any exploitation.	Obtain the latest software from the March Networks Partner Portal. In a web browser, enter the following: http://ip of recorder/setup. Log on to the recorder. On the Command Config main page, under Settings, click Upgrades. Or, use Command Enterprise (CES) to "push" updates automatically to all your recorders.	6700 recorders are shipped to customers with a default minimum ship level. This minimum ship level may be several versions behind the latest posted software.	Update 6700 recorder to the latest release found on the Partner Portal using the recorder's Command Config page or by way of Command Enterprise.	Update 6700 recorder to the latest release found on the Partner Portal using the recorder's Command Config page or by way of Command Enterprise.	Command Enterprise software is required for automation of software/firmware application to recorders.	Command Config or Command Client if using CES.	6700 Series Hybrid NVR Configuration Guide – Chapter 7 Configuring System Settings
6700 Communication Ports	Use secure https communication to access the device's web interfaces.	Communication over the default http port could be vulnerable to "sniffer attacks". When configuring sensitive information on the device, such as user accounts and passwords, access the recorder's Command Config web page using https.	Using Command Client, Log on directly to the recorder. Within the System tree, right–click on the recorder icon and select Open. Click Edit Addresses. Change the default ports 80 or 443 as required.	Communication over http and https is enabled by default on 6700 Series recorders.	Although you may not turn off the http access, you are able to change the port to something other than 80.	Choose your own port for https communication.	The customized https port must be "open" between the recorder and your computer in order to configure it.	Command Client	Command Professional or Single Recorder Client User Guide – Chapter 4 Managing Resources
6700 Admin Password	Create a strong password for the default admin account. March Networks' 6700 recorders allow you to create strong passwords as there are no restrictions to the number or type of characters used.	Never leave the default password blank. Create a strong password following the customer's password creation policies.	In a web browser, enter the following: http://ip of recorder/setup. Log on to the recorder. On the Command Config main page, under Users, click Profiles. Select Admin user and click Edit Selected User. Enter a password and click Ok.	March Networks 6700 Series recorders are shipped with the default admin account password set to (no password).	Change the admin account password on all your 6700 recorders to use the same strong password following the customer's password creation policies.	Change the admin account password on all your 6700 recorders to use individual strong passwords following the customer's password creation policies. Make use of identification Certificate to enhance Log on security.	With individual passwords per recorder, good password management becomes critical. A USB token or smartcard is required for Identification Certificates.	Command Config	6700 Series Hybrid NVR Configuration Guide – Chapter 4 Managing User Profiles
6700 User Accounts, Non-CES Managed Environment	When creating users accounts directly on the recorder, use strong passwords as per customer's password policy. Consider using secondary means of validation such as certificate or using Active Directory (LDAP).	Never leave a user account without a password.	In a web browser, enter the following: http://<recorder's IP address>/setup. Log on to the recorder. On the Command Config main page, under Settings, click Profiles. Select Add user and enter a username and password and click Ok.	Create strong password for each new local account. Assign the appropriate user profile with the correct permissions for the user.	Create strong password for each new local account. Assign the appropriate user profile with the correct permissions for user. Make use of identification Certificate to enhance Log on security.	Switch from local users to LDAP users in order to make use of Active Directory password policy.	LDAP must be in use on network.	Command Config	6700 Series Hybrid NVR Configuration Guide – Chapter 4 Managing User Profiles

Item ID	Item Description	Possible Vulnerability	How-To	Security Level 1 (default)	Security Level 2	Security Level 3	Security Level 3 Impact	Configured using...	Reference
6700 TimeSync NTP	Enable NTP time synchronization.	By leaving the automatic time sync disabled, the time of a device may drift which affects log files, making it difficult to track attacks.	In a web browser, enter the following: http://<recorder's IP address>/setup. Log on to the recorder. On the Command Config main page, under System, click Settings and then select System Time. Select NTP tab and enter the appropriate NTP information. Click Ok.	Time Synchronization is set to Manual. You may sync the time to your client computer.	Change Time Synchronization to use customer's NTP server.	Change Time Synchronization to use customer's NTP server.	NTP server must be in use on customer's network. Alternatively you may use an external (internet based) NTP server.	Command Config	6700 Series Hybrid NVR Configuration Guide – Chapter 7 Configuring System Settings
6700 Identification Certificate	Identification certificates are usually included in specific USB tokens or smartcards. Certificates can be linked to the 6700 Series Hybrid NVR Log on or to specific features. This adds an extra level of security between the recorder and the Client software.	None, adds extra level of security.	Insert the USB token/ smartcard containing the identification certificate into the client. In a web browser, enter the following: http://<recorder's IP address>/setup. Log on to the recorder. On the Command Config main page, under Users, click Certificates. Click the Server–>Available folder in the tree. Click the Add Certificate button and select a Certificate in the list. Click Ok.	Identification Certificates are disabled by default.	Enable identification certificate by obtaining (importing) one from USB token/ smartcard and saving it on the recorder and on the client.	Enable identification certificate by obtaining (importing) one from USB token/ smartcard and saving it on the recorder and on the client.	A USB token or smartcard is required. Cannot be used with LDAP/Active Directory users.	Command Config	6700 Series Hybrid NVR Configuration Guide – Chapter 6 Configuring Identification Certificates
COMMAND RECORDING SOFTWARE (CRS)									
CRS Server Security	Whether the server was supplied by the customer or purchased through March Networks as part of a Command Bundle, the server should be hardened following the CIS Microsoft Windows Server 2012R2 or later Benchmark guide.	Securing the CRS application will not be effective if the hardening process is not being applied to the server's Windows Operating system where CRS resides.	Use Remote Desktop to access the Server's Operating System and follow recommendations within the Windows Benchmark guide.	Windows Operating system is used as installed and configured on the server.	Perform hardening on the Server's OS as per CIS Microsoft Windows Server 2012 R2 or later Benchmark guide or customer's preferred benchmark guide.	Perform hardening on the Server's OS as per CIS Microsoft Windows Server 2012 R2 or later Benchmark guide or customer's preferred benchmark guide.	CRS software installation should be delayed until Windows Operating system Hardening is completed. If OS hardening is performed after the CRS installation, some firewall ports required by the CRS may be blocked, thus negatively impacting the CRS.	Windows Operating system.	CIS Benchmark guides https://learn.cisecurity.org/benchmarks

Item ID	Item Description	Possible Vulnerability	How-To	Security Level 1 (default)	Security Level 2	Security Level 3	Security Level 3 Impact	Configured using...	Reference
CRS Server Security, WDigest	Additional specific item to secure older Windows Server 2012 or Windows 8.	WDigest is used for LDAP and web-based authentication. It stores passwords in clear-text, in memory.	Use Remote Desktop to access the Server's Operating System and follow recommendations in reference. Apply Microsoft security update (KB2871997). Then, set the Use Logon-Credential entry in the Windows registry to a value of 0 (zero).	Windows Operating system is used as installed and configured on the server.	Perform hardening on the Server's OS as per reference.	Perform hardening on the Server's OS as per reference.	CRS software installation should be delayed until Windows Operating system Hardening is completed. If OS hardening is performed after the CRS installation, some firewall ports required by the CRS may be blocked, thus negatively impacting the CRS.	Windows Operating system.	https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2016/2871997
CRS Server Security, SMB service	Additional specific item to secure Windows Server 2012R2 or later. Please note that this service is not limited to file sharing, but control also active directory access (LDAP).	The SMB service running on port 445 may be left with signing not required.	Use Remote Desktop to access the Server's Operating System and follow recommendations in reference. We recommend to use the Local security Policy panel, use the registry key only as a second alternative."	Windows Operating system is used as installed and configured on the server.	Perform hardening on the Server's OS as per reference.	Perform hardening on the Server's OS as per reference.	CRS software installation should be delayed until Windows Operating system Hardening is completed. If OS hardening is performed after the CRS installation, some firewall ports required by the CRS may be blocked, thus negatively impacting the CRS.	Windows Operating system.	https://www.tenable.com/plugins/nessus/57608 https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-digitally-sign-communications-always
CRS Server Security, LDAP service	Additional specific item to secure Windows Server 2012R2 or later.	LDAP service running without enforcing encryption.	Use Remote Desktop to access the Server's Operating System and follow recommendations in reference.	Windows Operating system is used as installed and configured on the server.	Perform hardening on the Server's OS as per reference.	Perform hardening on the Server's OS as per reference.	CRS software installation should be delayed until Windows Operating system Hardening is completed. If OS hardening is performed after the CRS installation, some firewall ports required by the CRS may be blocked, thus negatively impacting the CRS.	Windows Operating system.	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190023
CRS Communication Ports	During the installation, you may change the default communication ports used between the Command Client and CRS to further secure access. You may also turn off http access.	When configuring sensitive information on the CRS, such as user accounts and passwords, access the CRS using https.	Using the Command Management Console, stop the server. Click the Change Server Settings button. Change the http or https ports. Click Save. Start the server.	By default, the ports used by CRS are: http 80 and https 443.	Although you may not disable http port 80, you may change it to something other than 80, forcing users to access CRS using https port 443.	Change the https port 443 to a custom port number. When working with remote CRS, use NAT Traversal communication which does not require inbound firewall ports to be opened at the CRS' location.	Custom port must be "open" between the CRS and client computer.	Command Management Console on the CRS Server	CRS Configuration Guide – Chapter 2 Installing Command Recording Software

Item ID	Item Description	Possible Vulnerability	How-To	Security Level 1 (default)	Security Level 2	Security Level 3	Security Level 3 Impact	Configured using...	Reference
CRS NAT Traversal Communication	NAT Traversal allows access to CRS and its camera streams without opening inbound firewall ports on the CRS' network and does not require the addition of specific routing rules. Note: if NAT Traversal is enabled, but ports remain open on the firewall, Clients will default to port based communication if the CRS responds on such ports.	Option 1 – If the CRS is not remote to your network, and there are no remote Clients requiring access to the CRS, you may disable the NAT Traversal feature. Option 2 – If you prefer to use NAT Traversal to allow access to a remote Client or remote CRS, especially to keep the CRS up-to-date with new software versions and patches, it is recommended to enable NAT Traversal communication. This type of connection uses Secure DTLS protocol for authentication and encryption between the Client and CRS.	Initiate a Remote desktop session to the CRS server. Option 1 – Using the Command Management Console, stop the CRS service. Click the Change Security Settings button. Select Disabled under NAT Traversal. Click Save. Start the CRS service. Option 2 – Using the Command Management Console, stop the CRS service. Click the Change Security Settings button. Select Enabled under NAT Traversal. Click Save. Start the CRS service.	On a new installation or upgrade of CRS, NAT Traversal is disabled by default. Note: Once enabled NAT Traversal communication will not be used by Clients unless enabled on the Command Enterprise, where the CRS must be registered, and the user is provided the NAT Traversal right within their profile.	Option 1 – If NAT Traversal is not required, it can be disabled using the Command Management Console. Option 2 – Make use of NAT Traversal	Option 1 – If NAT Traversal is not required, it can be disabled using the Command Management Console. Option 2 – Make use of NAT Traversal	When Command Client uses NAT Traversal communication with a CRS, the Client loses the ability of accessing the web page any IP device (IP cameras/ encoders) connected to that CRS.	Command Management Console on the CRS Server	CRS Configuration Guide – Chapter 3 – Getting started
CRS Admin Password	Create a strong password for the default admin account. March Networks CRS allows you to create strong passwords, as there are no restrictions on the number of characters used other than the following character: You may not use "$" in the password field.	Never leave the default password blank. Apply a strong password to the System Admin account following the customer's password creation policies.	Using Command Config, log on to the CRS. On the main page, under User Management, click Users. Select Admin user and click Edit Security Settings. Click Password Substitution and enter a password. Click Ok.	March Networks CRS software installs with the System Admin password left blank.	Set the same strong password for all CRS System admin account following the company's password creation policies.	Set strong individual passwords for the System Admin account on each CRS server on the network. Do so following the company's password creation policies. Add an identification certificate to enhance security.	With individual passwords per CRS, good password management becomes critical. A USB token or smartcard is required to add an identification certificate.	Command Config	CRS Configuration Guide – Chapter 5 Managing User Profiles
CRS Software Updates	Keep the CRS at the most up-to-date software version. Latest software is available for download from the March Networks Partner Portal. Subscribe to March Networks Security Updates and Advisories email alerts online to stay up-to-date.	The latest CRS software provides not only new features and bug fixes, but ensures any known vulnerabilities are addressed, preventing exploitations.	Using the Command Management Console, stop the server. Download the latest CRS software from the Partner Portal. Place the file directly on the server (using remote desktop) and launch the file. Follow the prompts.	CRS software CD is shipped to customers with a default minimum ship level. This may be several versions behind latest posted firmware.	Update CRS software to the latest release found on the Partner Portal.	Load latest CRS update file on Command Enterprise and update all CRS' automatically using CES' Mass Management feature.	Command Enterprise required for automation of software/firmware application.	Manually using upgrade file or using Command Enterprise	CRS Configuration Guide – Chapter 2 Installing Command Recording Software
CRS User Accounts, CRS Managed by CES	When a CRS is being managed by a CES, user accounts requiring access to the CRS should be created on the CES and authenticated by the CES.	Creating local CRS accounts when the CRS is being managed by a CES creates additional means of authentication and possible exploitation. Local accounts should be disabled (with the exception of the Admin account)	Using Command Config, log on to the CRS. On the Command Config main page, under User Management, click Users. Delete all local user accounts. Click Ok.	By default, only the admin password is created on a CRS. In a non-CES managed environment, local user account(s) would have been created.	Delete each local user account other than the admin account. Note: If using SiteManager or Decode Station, a local user on CRS must remain to allow those applications direct local access.	Delete each local user account other than the admin account. Note: If using SiteManager or Decode Station, a local user on CRS must remain to allow those applications direct local access.	None	Command Config	CRS Configuration Guide – Chapter 5 Managing User Profiles

Item ID	Item Description	Possible Vulnerability	How-To	Security Level 1 (default)	Security Level 2	Security Level 3	Security Level 3 Impact	Configured using...	Reference
CRS User Accounts, Non-CES Managed Environment	When creating users accounts, use strong passwords as per customer's password policy. Enable User profile security settings (Password substitution, expiration date and change password on...) for each user. Consider using secondary means of validation, such as certificate, or you may use LDAP.	Without the User profile Security settings enabled, local user passwords are created and never changed/ updated, exposing potential security issue.	Using Command Config, log on to the CRS. On the Command Config main page, under User Management, click Users. Select a user and click Edit Security Settings. Enable the Security settings as required. Click Ok.	By default, User profile security settings are disabled for local users	For each local user profile, enable the Password substitution, Profile Expiration Date and Change password on settings.	Switch from local users to LDAP users in order to make use of Active Directory password policies. This also ensures your user credentials are stored in a single location.	LDAP must be in use on network.	Command Config	CRS Configuration Guide – Chapter 5 Managing User Profiles
CRS MaxUser Connection	Set the Max Simultaneously Connected Users setting to the number of actual users accessing the system (including administrator) to prevent access attempts by non-authorized users. When all authorized users are connected, no other Log on attempts are permitted.	By leaving the default setting in place, unauthorized users may access the Log on page and try to gain access to the system.	Using Command Config, log on to the CRS. On the main page, under General Settings, click System. Under Users, set the Max Simultaneously Connected Users count. Click Save Changes.	By default, the Max Simultaneously Connected Users is set to 32 users/clients.	Set the Max Simultaneously Connected Users setting to the number of actual users accessing the system.	Set the Max Simultaneously Connected Users setting to the number of actual users accessing the system.	The Max Simultaneously Connected Users setting needs to be updated for all new client users added to the system.	Command Config Web page	CRS Configuration Guide – Chapter 8 Configuring System Settings
CRS Identification Certificate	You can enhance the security of the CRS by adding identification certificates. Identification certificates are included in specific USB tokens or smartcards. Certificates can be linked to the CRS connection (via Command Config, Command Client or to specific features). This adds an extra level of security between the CRS and client user.	None. Adds extra level of security.	Insert the USB token/ smartcard containing the identification certificate into the client. In a web browser, enter the following: http://ip of CRS/setup. Log on to the CRS. On the Command Config main page, under User Management, click Certificates. Click Import. Select a Certificate in the list and click Ok. Click Save Changes.	Identification Certificates are disabled by default.	Enable identification certificate by obtaining (importing) one from USB token/ smartcard and saving it on the CRS and on the client.	Enable identification certificate by obtaining (importing) one from USB token/ smartcard and saving it on the CRS and on the client.	A USB token or smartcard is required. Cannot be used with LDAP/Active Directory users.	Command Config Web page	CRS Configuration Guide – Chapter 7 Configuring Identification Certificates

Item ID	Item Description	Possible Vulnerability	How-To	Security Level 1 (default)	Security Level 2	Security Level 3	Security Level 3 Impact	Configured using...	Reference
COMMAND ENTERPRISE (CES), ALSO INCLUDES SEARCHLIGHT AND COMMAND FOR TRANSIT									
CES Server Security	The server selected to host the CES software should be hardened following the CIS Microsoft Windows Server 2012 R2 or later Benchmark guide.	Securing the CES application will not be effective if the hardening process is not being applied to the server's Windows Operating system where CES resides.	User Remote Desktop to access the Server's Operating System and follow recommendations within the Windows Benchmark guide.	Windows Operating system is used as installed and configured on the server.	Perform hardening on the Server's OS as per CIS Microsoft Windows Server 2012 R2 or later Benchmark guide, or customer's preferred benchmark guide.	Perform hardening on the Server's OS as per CIS Microsoft Windows Server 2012 R2 or later Benchmark guide, or customer's preferred benchmark guide.	CES software installation should be delayed until Windows Operating system Hardening is completed. If OS hardening is performed after the CES installation, some firewall ports required by the CES may be blocked, negatively impacting the CES.	Windows Operating System	CIS Benchmark guides https://learn.cisecurity.org/benchmarks
CES Server Security, SMB service	Additional specific item to secure Windows Server 2012R2 or later. Please note that this service is not limited to file sharing, but control also active directory access (LDAP).	The SMB service running on port 445 may be left with signing not required.	Use Remote Desktop to access the Server's Operating System and follow recommendations in reference. We recommend to use the Local security Policy panel, use the registry key only as a second alternative.	Windows Operating system is used as installed and configured on the server.	Perform hardening on the Server's OS as per reference.	Perform hardening on the Server's OS as per reference.	CES software installation should be delayed until Windows Operating system Hardening is completed. If OS hardening is performed after the CES installation, some firewall ports required by the CES may be blocked, negatively impacting the CES.	Windows Operating system.	https://www.tenable.com/plugins/nessus/57608 https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-digitally-sign-communications-always
CES Server Security, LDAP service	Additional specific item to secure Windows Server 2012R2 or later.	LDAP service running without enforcing encryption.	Use Remote Desktop to access the Server's Operating System and follow recommendations in reference. Follow CES Install Guide advice, and select SSL/TLS connections with SIMPLE binding.	Windows Operating system is used as installed and configured on the server.	Perform hardening on the Server's OS as per reference.	Perform hardening on the Server's OS as per reference.	CES software installation should be delayed until Windows Operating system Hardening is completed. If OS hardening is performed after the CES installation, some firewall ports required by the CES may be blocked, negatively impacting the CES.	Windows Operating system.	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190023
CES Communication Ports	During the installation, you may change the default communication ports used between the Command Client and CES to further secure access.	When configuring sensitive information on the CES, such as user accounts and passwords, access the CES using https.	Initiate a Remote desktop session to the server. Using the Enterprise Console, stop the server. Click the NETWORKS tab. Change the http and https settings as required. Click Save. Start the server.	By default, the ports used by CES are: http 80 and https 443.	Although in the current version you may not disable http port 80, you may change it to something other than 80.	You may change both port 80 and 443 to alternate port numbers.	Custom port numbers must be "open" between the CES and client computer.	Command Enterprise Console on the CES Server	Command Enterprise and Client Installation Guide – Chapter 3 Installing Command Enterprise

Item ID	Item Description	Possible Vulnerability	How-To	Security Level 1 (default)	Security Level 2	Security Level 3	Security Level 3 Impact	Configured using...	Reference
Configure TLS 1.2 as minimum version	TLS 1.2 can be enforced as the minimum allowed version.	The default setting is TLS 1.0, to support backwards compatibility with 3000, 4000 and 8000 recorders at version below 5.8, and with 5000 recorders.	Configure the Min. TLS version to TLS 1.2, in the Command Enterprise console. Please refer to the Command Enterprise Installation Guide, in the "Network Tab" section.	Set this to TLS 1.2 if you don't need to support old recorders version.	Set this to TLS 1.2, and update your recorders in necessary.	Set this to TLS 1.2, and update your recorders in necessary.	Same as other levels, older versions of recorders need to be updated to preserve compatibility.	Command Enterprise Console on the CES Server	Command Enterprise and Client Installation Guide – Chapter 3 Installing Command Enterprise
HTTPS video streaming	This parameter control the encryption in transmission of media sent to clients. This parameter is set to true to new installation of CES, and preserved as false when upgrading it from a release prior to 2.7.	"Without enabling this, media will be sent in clear to clients. Depending on the security of the network, you may desire to avoid this."	Configure the secure_ streaming_enabled parameter to true, in the Command Enterprise console. Please refer to the Command Enterprise Installation Guide, in the "Advanced Tab" section.	This parameter is set to TRUE only on new installations and FALSE with upgrades from previous versions.	Set parameter to TRUE.	Set parameter to TRUE.	Same as other levels, recorders will use more computational resources to stream video.	Command Enterprise Console on the CES Server	Command Enterprise and Client Installation Guide – Chapter 3 Installing Command Enterprise
CES and Device Info Security Level	These parameters control how CES and recorders authorize access to informational pages.	Informational pages publish service and recorder addresses, and their version.	Configure these parameters to "Authentication", to require authentication to access to informational pages. Please refer to the Command Enterprise Installation Guide, in the "Network Tab" section.	Set this to "Authentication" if you don't need to support old Command SDK integrations.	Set this to "Authentication", and update any old Command SDK integration.	Set this to "Authentication", and update any old Command SDK integration.	Third party application based on the Command SDK may need an update to the Command SDK 2.10, to ensure compatibility. Access to the recorder's https:// <ip of device> /public/ index.htm page will require authentication, and a user with proper access rights.	Command Enterprise Console on the CES Server	Command Enterprise and Client Installation Guide – Chapter 3 Installing Command Enterprise
CES NAT Traversal Communication	You may enable NAT Traversal communication between CES authenticated clients and CES registered recording devices. This allows Clients a connection to a recording device, without opening inbound firewall ports on the recording device's network or the requirement for additional specific routing rules.	Option 1 – If you do not have Clients or recording devices remote to your network, you may disable NAT Traversal communication globally within CES. Option 2 – If you prefer to use NAT Traversal to allow access to a remote Client or remote recording device, especially to keep this device up-to-date with new software versions and patches, it is recommended to enable NAT Traversal communication. This type of connection uses Secure DTLS protocol for authentication and encryption between the Client and March Networks supported recording devices.	Initiate a Remote desktop session to the CES server. Using the Enterprise Console, stop Command Enterprise. Click the NAT Traversal tab. Enable/ Disable NAT Traversal as required. If enabling, choose between the internal STUN server or provide one or more IP addresses for external STUN/TURN server(s). Click Save. Start Command Enterprise. Log on to the CES using Command Client and enable NAT Traversal right for required user profiles.	By default, NAT Traversal communication is disabled on the CES and will not be used by any authenticated Clients even if the NAT Traversal feature was enabled on a registered recording device.	Option 1 – Leave NAT Traversal disabled on the CES Option 2 – Enable NAT Traversal communication using local STUN or provide IP address for external STUN/TURN server. Enable Remote Provisioning (SSH) to 8000/9000/RideSafe recorders for specific users only.	Option 1 – Leave NAT Traversal disabled on the CES Option 2 – Enable NAT Traversal communication using local STUN or provide IP address for external STUN/TURN server. Leave Remote Provisioning option disabled for all users.	By using NAT Traversal communication, a Client loses the ability of accessing an IP device's web page. When the Remote Provisioning right is not granted to a CES user profile, and a Client's IP address is not entered within the Enterprise Console's NAT Traversal tab, accessing the Provisioning Interface of any remote recorder will not be possible over a NAT Traversal connection.	Command Enterprise Console on the CES Server as well as Command Client.	Command Enterprise and Client Installation Guide – Chapter 3 Installing Command Enterprise Command Enterprise and Client User Guide – Chapter 4 Managing User Profiles

Item ID	Item Description	Possible Vulnerability	How-To	Security Level 1 (default)	Security Level 2	Security Level 3	Security Level 3 Impact	Configured using...	Reference
CES SuperAdmin Password	Create a strong password for the Superadmin account during installation. March Networks CES allows you to create strong passwords as there are no restrictions on the number or type of characters used. Don't share the superadmin account credentials and use this account only for very limited installation and recovery tasks.	March Networks CES software installs with the Superadmin password "not set".	Remote desktop to the server. Using the Enterprise Console, stop the Command Enterprise. Click the SUPERADMIN tab. Set a strong password for this user or enable and link it to an LDAP/Active Directory user. Click Save and start Command Enterprise.	Apply a strong password to the Superadmin account following the customer's password creation policies.	Apply a strong password to the Superadmin account following the customer's password creation policies or, link the SuperAdmin to an LDAP user. Create a secondary Admin account for everyday use. Only use the Superadmin account for installation/ recovery purposes going forward.	Link the SuperAdmin to an LDAP user in order to enforce user password complexity restrictions and regular password changes. Create a secondary Admin account for everyday use. Only use the Superadmin account for installation/ recovery purposes going forward.	LDAP must be in use on the network to link the Superadmin account to an Active Directory user.	Command Enterprise Console on the CES Server	Command Enterprise and Client Installation Guide – Chapter 3 Installing Command Enterprise
CES ExtSQL Secure	When using a Microsoft SQL Server 2008, 2012, or 2014 as the external database for CES/Searchlight, instead of the pre-configured Microsoft SQL Server Express 2012 included with Command Enterprise, you should be following the recommendations of the CIS Microsoft SQL 2008 R2 or 2012 or 2014 Benchmark guide in hardening that product before the CES is rolled out.	None. Adds extra level of security.	User Remote Desktop to access the Server's Operating System, where the external SQL database was installed, and follow the recommendations within the Microsoft SQL Benchmark guide.	SQL Server is used as installed and configured.	Perform hardening on the SQL server as per the CIS Microsoft SQL 2008 R2 or 2012 or 2014 Benchmark guide or customer's IT preferred benchmark guide before the installation of CES.	Perform hardening on the SQL server as per the CIS Microsoft SQL 2008 R2 or 2012 or 2014 Benchmark guide or customer's IT preferred benchmark guide before the installation of CES.	CES software installation should be delayed until SQL Server Hardening is completed.	SQL Software and Windows Operating System	CIS Benchmark guides https://learn.cisecurity.org/benchmarks
CES Software Updates	Keep the CES at the most up-to-date software version. Latest software is available for download from the March Networks Partner Portal. Subscribe to March Networks Security Updates and Advisories email alerts online to stay up-to-date.	The latest CES software provides not only new features and bug fixes, but ensures any known vulnerabilities are addressed, preventing exploitations.	Using the Enterprise Console, stop the server. Download the latest CES software from the Partner Portal. Place the file directly on the server (using remote desktop) and launch the file. Follow the prompts to install/update the current software.	CES software CD is shipped to customers with a default minimum ship level. This may be several versions behind latest posted firmware.	Update CES software to the latest release found on the Partner Portal.	Load latest CRS/ recorder update file(s) on Command Enterprise and update all recording devices automatically using CES' Mass Management feature.	Command Enterprise required for automation of software/firmware application.	Command Client authenticated to CES	Command Enterprise and Client Installation Guide – Chapter 3 Installing Command Enterprise

Item ID	Item Description	Possible Vulnerability	How-To	Security Level 1 (default)	Security Level 2	Security Level 3	Security Level 3 Impact	Configured using...	Reference
CES User Accounts	When creating user accounts, use strong passwords as per customer's password policy. You may also enable the Force Password change at next log on. Make use of the CES' Password Policy of minimum length, case sensitivity, number and special character use. Consider using secondary means of validation such as certificate or using LDAP.	Never leave a user account without a password. Plan the assignment of all user rights carefully as some rights, (such as User Management & Remote Provisioning) allow a user to receive SuperAdmin privileges.	Using Command Client, Log on directly to the CES. From the Main Menu, select User Management. Click the Users tab and select a user to change a password.	Create strong password for each new local account. Assign the appropriate user profile with the correct permissions for the user.	Create strong password for each new local account. Assign the appropriate user profile with the correct permissions for user. Make use of identification Certificate.	Switch from local users to LDAP users in order to make use of Active Directory password policies. This also ensures your user credentials are stored in a single location. Local user accounts should be disabled. SuperAdmin account should use LDAP.	LDAP must be in use on the network. Recording device re-registration may be required if local CES account was used during registration process.	Command Client authenticated to CES	Command Enterprise and Client User Guide – Chapter 5 Managing User Accounts
CES Password Policy	CES' Password Policy enforces minimum password length, case sensitivity, number and special character use, as well as a password expiry for all new local accounts created. Consider using secondary means of validation such as certificate or using LDAP instead of local accounts.	Without enabling the CES' Password Policies, user accounts can be created with blank or weak passwords containing as little as one character.	Initiate a Remote desktop session to the server. Using the Enterprise Console, stop the server. Click the Password Policy tab. Enable the various policies as per the customer's own password policy requirements.	CES Password Policies are disabled by default.	Enable the various policies as per the customer's own password policy requirements.	Switch from local users to LDAP users in order to make use of Active Directory password policies. This also ensures your user credentials are stored in a single location. Local user accounts should be disabled. SuperAdmin account should use LDAP.	LDAP must be in use on the network. Recording device re-registration may be required if local CES account was used during registration process.	Enterprise Console on the CES Server	Command Enterprise and Client Installation Guide – Chapter 3 Installing Command Enterprise
CES Identification Certificate	You can enhance the security of Command Enterprise by adding USB token or smart card user certificates. Authentication certificates are linked to a user's Command Enterprise Log on connection and optionally to session authentication. The certificate is required to authenticate the user credentials. This adds an extra level of security between the CES and local client user.	None. Adds extra level of security.	Using Command Client, Log on directly to the CES. From the Main Menu, select User Management. Click Manage Certificates from the Users tab.	Identification Certificates are disabled by default.	Enable identification certificate by obtaining (importing) one from USB token/ smartcard and saving it on the CES and on the client.	Enable identification certificate by obtaining (importing) one from USB token/ smartcard and saving it on the CES and on the client.	A USB token or smartcard is required. Cannot be used with LDAP/Active Directory users.	Command Client authenticated to CES	Command Enterprise and Client User Guide – Chapter 5 Managing User Accounts

Item ID	Item Description	Possible Vulnerability	How-To	Security Level 1 (default)	Security Level 2	Security Level 3	Security Level 3 Impact	Configured using...	Reference
CES LDAP Connection	Enable LDAP as a means to enforce user password complexity restrictions and regular password changes and to store your user passwords in one location.	Local accounts may not meet company minimum policy on password complexity restrictions and/ or regular password changes as well as being stored locally on each server.	Initiate a Remote desktop session to the server. Using the Enterprise Console, stop the server. Click the LDAP Services tab. Select LDAP Enabled. Enter the required LDAP server information. Select Digest as Binding Type and StartTLS for Secure (SSL). Click Verify. Start the server.	LDAP is off by default.	Enable a connection to the LDAP server on the network for all regular user accounts. Continue to allow local account creation for administration account purposes.	Enable a connection to LDAP server on the network. Disallow all Local User accounts by selecting the Disable Local Users option.	All users must have an account on the LDAP server. All recording devices and applications, like Command Center, which may have been using a local CES user account for connection to the CES, must have their configuration updated to use new CES LDAP account(s).	Command Enterprise Console on the CES Server	Command Enterprise and Client Installation Guide – Chapter 3 Installing Command Enterprise
EDGE DEVICES (IP CAMERAS AND ENCODERS)									
EDGE Defaults	If you are not working with a brand new Edge device, start by resetting the device to manufacturer's defaults.	If a device is not brand new out of the box, a previous configuration may expose vulnerabilities. Start with a known default configuration before configuring the device.	Refer to the particular camera's configuration guide	All new products are shipped with manufacturer's default settings.	Apply manufacturer's default settings before configuring a device not recently purchased from the manufacturer.	Apply manufacturer's default settings before configuring a device not recently purchased from the manufacturer.	When applying manufacturer settings, all current settings on device will be lost.	Internet Browser	Specific camera model # Configuration Guide
EDGE Firmware Upgrade	Keep the EDGE device at the most up-to-date software version. Latest software is available for download from the March Networks Partner Portal. Subscribe to March Networks Security Updates and Advisories email alerts online to stay up-to-date.	The latest Edge device firmware provides not only new features and bug fixes, but ensures any known vulnerabilities are addressed, preventing exploitations.	Refer to the particular camera's configuration guide	Edge devices are shipped to customers with a default minimum ship level which may differ based on model of device. This minimum ship firmware may be several versions behind latest posted firmware.	Update Edge Devices to the latest release found on the Partner Portal using Camera's configuration page or Command Enterprise.	Load latest Edge Devices firmware file on Command Enterprise and update all devices automatically using CES' Mass Management feature.	Command Enterprise required for automation of software/firmware application.	Internet Browser	Specific camera model # Configuration Guide
EDGE Communication	Use secure https communication to access the device's web interface.	Communication over the default http port could be vulnerable to "sniffer attacks". When configuring sensitive information on the device, such as user accounts and passwords, access the web configuration page using https.	Refer to the particular camera's configuration guide. For Edge OS II cameras, http and https settings must be changed from their Command Client page.	Communication over http and https is enabled by default on the majority of Edge Devices.	If http cannot be disabled on a particular Edge device, replace the value 80 with another value of your choice to eliminate communication over port 80.	Change port 443 to another port of your choice.	The customized https port must be "open" between the Edge device and your Client computer in order to configure it. This port must also be provided to the recording device in order for it to connect to the Edge Device.	Internet Browser	Specific camera model # Configuration Guide

Item ID	Item Description	Possible Vulnerability	How-To	Security Level 1 (default)	Security Level 2	Security Level 3	Security Level 3 Impact	Configured using...	Reference
EDGE Admin Password	Create a strong password for the default admin account. March Networks Edge devices allow you to create strong passwords as there are no restrictions on the number or type of characters used.	March Networks Edge Devices manufactured after January 1, 2020 and running firmware version 1.0.8 will be programmed to request a default password change at first login. Never leave the default password blank. Apply a strong password to the device following the customer's password creation policies.	Refer to the particular camera's configuration guide	March Networks Edge Devices manufactured after January 1, 2020 and running firmware version 1.0.8 will be programmed to request a default password change at first login. Previous devices were shipped with the default admin account password set to: (no password).	Change the password on all Edge devices to use the same strong password following the customer's password creation policies.	Change the password on all Edge devices to their own individual strong password following customer's password creation policies. Make use of identification Certificate to enhance Log on security.	With individual passwords per Edge device, good password management becomes critical.	Internet Browser	Specific camera model # Configuration Guide
EDGE User Accounts	Disable additional local user accounts. Keep only local admin account configured with a strong password as per customer's password policy.	Disable all additional user accounts, as they may allow unauthorized entry.	Refer to the particular camera's configuration guide	Only the admin account is active. Configure a strong password as per customer's password policy.	Ensure no other user accounts have been created. Provide admin account to any recorder in order to add the Edge device.	Ensure no other user accounts have been created. Provide admin account to any recorder in order to add the Edge device.	None	Internet Browser	Specific camera model # Configuration Guide
EDGE TimeSync NTP	Enable NTP time synchronization when devices are not connected to recorder's camera network interface.	By leaving the time sync to the default "manual", the time of a device may drift, which affects log files and makes it difficult to track attacks.	Refer to the particular camera's configuration guide	Time Synchronization is set to manual.	Time Synchronization is changed to use customer's NTP server if device is not connected to a recorder's camera network interface.	Time Synchronization is changed to use customer's NTP server if device is not connected to a recorder's camera network interface.	In order to use NTP, the Edge device cannot be connected to the recorder's camera network interface.	Internet Browser	Specific camera model # Configuration Guide
EDGE Services Protocols	Disable any unused services and protocols such as Audio i/o or Auxiliary i/o.	An enabled service may provide a user with unauthorized access to audio streams and control of alarms and relays.	Refer to the particular camera's configuration guide	Audio talk channel and Aux i/o are enabled by default.	Disable any unused audio and Aux services.	Disable any unused audio and Aux services.	None	Internet Browser	Specific camera model # Configuration Guide
EDGE Streamers	Secure RTP/Mjpeg streams or disable them altogether.	Users may request video streams and view video from a device using its default username/password.	Refer to the particular camera's configuration guide	RTP unicast streams are enabled by default.	Ensure RTP streams are secured by disabling "Allow anonymous users" and ensuring a "strong" password was set for the device.	Disable both RTP and Mjpeg streams.	None	Internet Browser	Specific camera model # Configuration Guide
EDGE Identification Certificate	Certificates can be linked to the Edge device Log on or to specific features depending on device model. This adds an extra level of security between the Edge Device and the recorder.	None. Adds extra level of security.	Refer to the particular camera's configuration guide	Identification Certificates are disabled by default.	Enable identification certificate by obtaining (importing) one from USB token/ smartcard and saving it on the Edge device and on the client.	Enable identification certificate by obtaining (importing) one from USB token/ smartcard and saving it on the Edge device and on the client.	A USB token or smartcard is required.	Internet Browser	Specific camera model # Configuration Guide
EDGE 802.1x	Enable 802.1x security protocol to authenticate the device after a connection to a switch, granting or denying them access to the network.	None. Adds extra level of security.	Refer to the particular camera's configuration guide	802.1x is disabled by default.	Enable 802.1x by adding the CA certificate, public and private key.	Enable 802.1x by adding the CA certificate, public and private key.	Customer network equipment must support 802.1x protocol.	Internet Browser	Specific camera model # Configuration Guide

The document is a configuration hardening guide to identify security vulnerability exposures associated with the configuration of March Networks products. A failure to follow March Networks recommendations or industry best practices associated with device configuration may increase the risk associated with security vulnerabilities. The security of a CCTV network is the dependent on the entire ecosystem, including device manufacturers, integrators, service providers, as well as the end user organization. March Networks cannot guarantee that our products will be free from viruses and/or security vulnerabilities. March Networks shall not be responsible nor liable for any damages, including direct, indirect or consequential in connection with this guide. This guide is only to be used for its intended purpose.

North America 1 800 563 5564
Latin America . . . . . +5255 5259 9511
Europe . . . . . +39 0362 17935

Asia . . . . . +65 6818 0963
Australia and New Zealand . . . . . +61 1300 089 419
Middle East and Africa . . . . . +971 4 399 5525

© 2021 March Networks. All rights reserved. Information in this document is subject to change without notice. MARCH NETWORKS, March Networks Command, March Networks Searchlight, March Networks RideSafe, and the MARCH NETWORKS logo are trademarks of March Networks Corporation. All other trademarks are the property of their respective owners. 060-3350-00-G