National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

MAGNUM-HW-C-CC, Version 1.0

Report Number: CCEVS-VR-11022-2020

Dated: 01/10/2020

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

Sheldon Durrant: Senior Validator

John Butterworth: Lead Validator

Lisa Mitchell: ECR Team

Clare Olin: ECR Team

Common Criteria Testing Laboratory

Kathleen Moyer

Brad Mitchell

Thibaut Marconnet

Heather Hazelhoff

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the MAGNUM-HW-C-CC Series Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in November 2019. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for Collaborative Protection Profile for Network Devices, v2.1 (CPP_ND_V2.1).

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the Collaborative Protection Profile for Network Devices, v2.1 (CPP_ND_V2.1). This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations.
Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Collaborative Protection Profile for Network Devices, v2.1 (CPP_ND_V2.1) containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	MAGNUM-HW-C-CC
Protection Profile	CPP_ND_V2.1
Security Target	MAGNUM-HW-C-CC Security Target
Evaluation Technical Report	Evertz MAGNUM NDcPP v2.1 ETR
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Evertz Microsystems Ltd.
Developer	5292 John Lucas Drive Burlington, Ontario CANADA
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	John Butterworth: Lead Validator

	Sheldon Durrant: Senior Validator

3 Architectural Information

3.1 TOE Product Type

The TOE is classified as a network device (a generic infrastructure device that can be connected to a network). The TOE hardware device is the Evertz MAGNUM-HW-C-CC which includes the MAGNUM-HW-C-CC (1 RU) running MAGNUM firmware v19.10.1. The MAGNUM-HW-C-CC serves as the primary user and network interface device for the MAGNUM control application.

3.2 TOE Usage

Evertz MAGNUM software is a custom-developed application written primarily in python. MAGNUM operates as a combination of an application layer and as part of the integrated Linux platform stack, using a customized Linux distribution. The TOE version of MAGNUM is only operable on Evertz-provided platforms and hardware.

MAGNUM serves as the control interface for Evertz's proprietary IPX media streaming switch fabric that allows the general user to establish, change, and tear down multicast IP video streams. MAGNUM may also serve as a general control interface for similar Evertz and third-party systems and devices.

Equipment to prepare video for IP transport, or to convert it into other video formats, is outside the scope of this TOE. Such equipment includes, but is not limited to, cameras, KVMs, codecs, video servers and video displays. Equipment to perform functions such as embedding audio and/or other information within the video stream is also outside the scope of this TOE.

The TOE is an infrastructure network device that provides secure remote management, auditing, and updating capabilities. The TOE provides secure remote management using an HTTPS/TLS web interface and an SSH command line interface. The TOE generates audit logs and transmits the audit logs to a remote syslog server over a mutually authenticated TLS channel. The TOE verifies the authenticity of software updates by verifying the digital signature prior to installing any update.

The scope of the evaluated functionality includes the following,

- Secure remote administration of the TOE via TLS and SSH
- Secure Local administration of the TOE
- Secure connectivity with remote audit servers
- Secure access to the management functionality of the TOE
- Identification and authentication of the administrator of the TOE

No other functionality is included within the scope of this evaluation.

MAGNUM issues commands (via dedicated internal API) to Evertz's proprietary IPX switching fabric and other production endpoints for the purpose of initiating, maintaining, and tearing down virtual routing paths. The MAGNUM-HW-C-CC device serves as the primary operational and administrative management interface to the closed multicast switching environment.

Users and administrators may access MAGNUM software via direct connection using a terminal session. Administrators only may access MAGNUM via a dedicated management workstation operating over an Out-of-Band Management (OOBM) network. Sites may close this OOBM network or may operate MAGNUM within an existing OOBM, as long as the topology is compliant with the security parameters listed below.

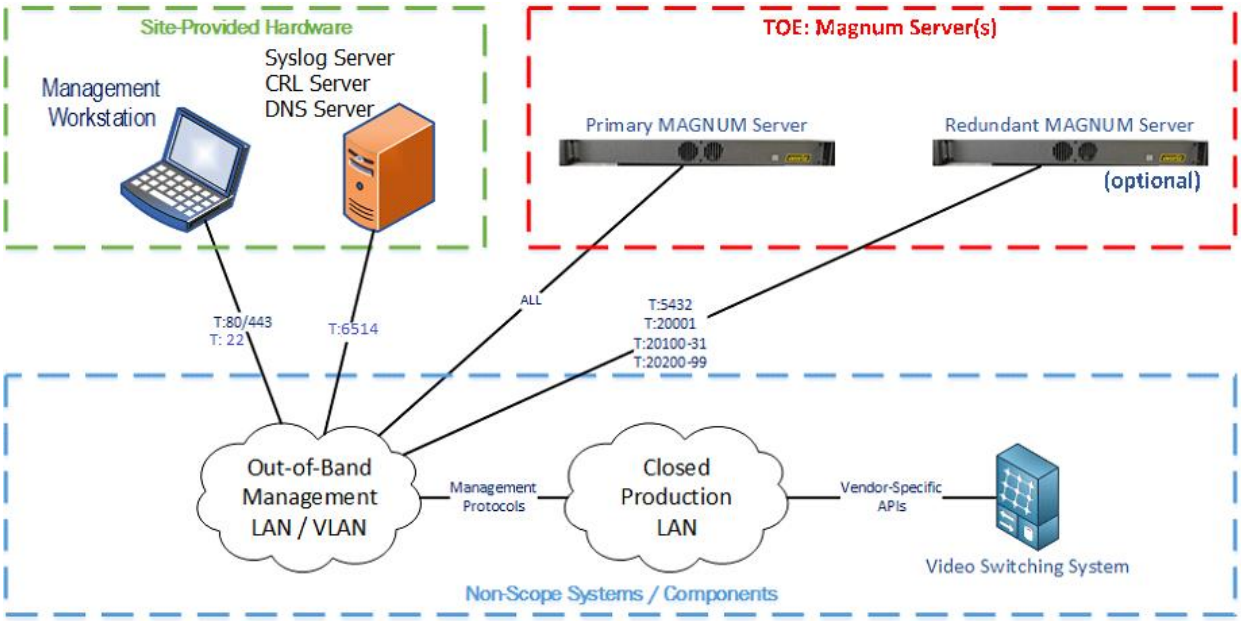

Figure 1 TOE Topology

4 Security Policy

4.1 Logical Scope of the TOE

The figure below depicts the logical scope of the TOE.

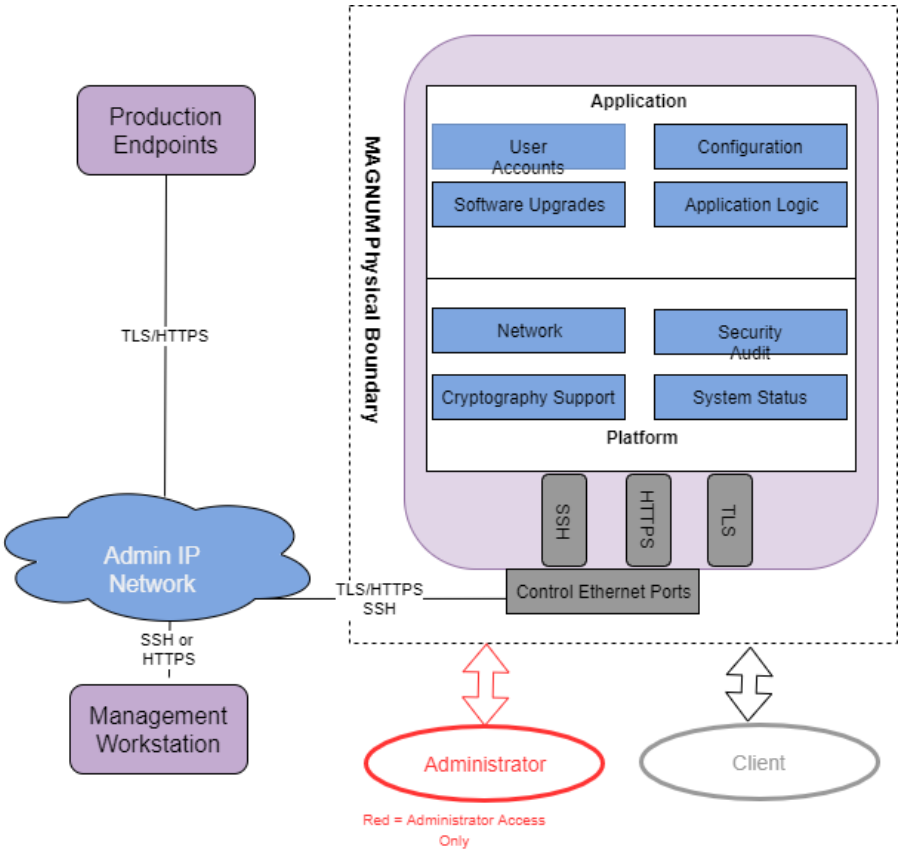

Figure 2 TOE Logical Scope and Workflow

The TOE supports the following functionality:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

4.2 Security Functions provided by the TOE

The TOE provides the security functionality required by NDcPP v2.1.

4.2.1 Security Audit

The TOE generates audit records for security relevant events. Audit data are stored internally and are only accessible to privileged administrators. The TOE supports role-based access control (RBAC) for authentication and authorization to management and security functions.

The TOE also supports sending audit records to a remote Syslog server. Audit records sent to the remote server are protected by a TLS connection. Each audit record includes identity (username, IP address, or process), date and time of the event, type of event, and the outcome of the event.

4.2.2 Cryptographic Support

The TOE includes an OpenSSL library that implements CAVP validated cryptographic algorithms for random bit generation, encryption/decryption, authentication, and integrity protection/verification. These algorithms are used to provide security for the TLS, HTTPs, and SSH connections for secure management and secure connections to a syslog and authentication servers. TLS and HTTPs are also used to verify firmware updates. The cryptographic services provided by the TOE are described below.

Cryptographic Protocol	Use within the TOE
HTTPS/TLS (client)	Secure connection to syslog FCS_HTTPS_EXT.1, FCS_TLSC_EXT.2
HTPS/TLS (server)	Peer connections to a backup MAGNUM and remote management FCS_HTTPS_EXT.1, FCS_TLSS_EXT.1
SSH(server)	Remote management FCS_SSHS_EXT.1
AES	Provides encryption/decryption in support of the TLS and SSH protocol. FCS_TLSC_EXT.2, FCS_TLSS_EXT.1, FCS_SSHS_EXT.1
DRBG	Deterministic random bit generation use to generate keys. FCS_TLSS_EXT.1, FCS_RBG_EXT.1, FCS_SSHS_EXT.1
Secure hash	Used as part of digital signatures and firmware integrity checks. FCS_COP.1/Hash, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1
HMAC	Provides keyed hashing services in support of TLS. FCS_COP.1/KeyedHash, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1
EC-DH	Provides key establishment for TLS. FCS_CKM.2, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1
ECDSA	Used to generate EC-DH components for key establishment for TLS. FCS_CKM.1, FCS_TLSS_EXT.1
RSA	Provide key generation and signature generation and verification (PKCS1_V1.5) in support of TLS. FCS_CKM.1, FCS_COP.1/SigGen, FCS_COP.1/SigVer, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1

Table 1 TOE Cryptographic Protocols

Each of these cryptographic algorithms have been validated for conformance to the requirements specified in their respective standards, as identified below.

Algorithm	Standard	CAVP Certificate #	Processors
AES 128/256-bit CBC, CTR, GCM	IOS 19772 (GCM) IOS 10116(CTR)	C1168	Intel® Xeon® D-1541
CTR DRBG using AES 256	ISO/IEC 18031:2011	C1168	Intel® Xeon® D-1541
EC-DH	NIST SP 800-56A (key establishment)	C1168	Intel® Xeon® D-1541
ECDSA with NIST	FIPS PUB 186-4, “Digital Signature	C1168	Intel® Xeon® D-1541

Algorithm	Standard	CAVP Certificate #	Processors
curves P-256, P384	Standard (DSS), Appendix B.4		
HMAC-SHA-1/256/384/512	ISO/IEC 9797-2:2011	C1168	Intel® Xeon® D-1541
SHA-1/256/384/512	ISO/IEC 10118-3:2004	C1168	Intel® Xeon® D-1541
RSA 2048-, 3072-, 4096-bit	FIPS PUB 186-4 (key generation)	C1168[1]	Intel® Xeon® D-1541
RSA 2048-, 3072-, 4096-bit	ISO/IEC 9796-2 (digital signature generation and verification)	C1168	Intel® Xeon® D-1541

Table 2 CAVP Algorithm Testing References

4.2.3 Identification and Authentication

The TOE authenticates administrative users using a username/password combination. The TOE does not allow access to any administrative functions prior to successful authentication. The TOE validates and authenticates X.509 certificates for all certificate uses.

The TOE supports passwords consisting of alphanumeric and special characters and enforces minimum password lengths. The TSF supports certificates using RSA signature algorithms. Certificates are used to authenticate trusted channels, not administrators. The TOE only allows users to view the login warning banner prior to authentication. Remote administrators are locked out after a configurable number of unsuccessful authentication attempts.

4.2.4 Security Management

The TOE allows users with the Security Administrator role to administer the TOE over a remote web UI, remote CLI, or a local CLI. These interfaces do not allow the Security Administrator to execute arbitrary commands or executables on the TOE. Security Administrators can manage connections to an external Syslog server, as well as determine the size of local audit storage.

4.2.5 Protection of the TSF

The TOE implements several self-protection mechanisms. This protection includes self-tests to ensure the correct operations of cryptographic functions. Firmware upgrades, performed by a Security Administrator, must pass two authentication tests. The TOE does not provide an interface for the reading of secret or private keys. The TOE ensures timestamps, timeouts, and certificate checks are accurate by maintaining a real-time clock.

4.2.6 TOE Access

The TOE can be configured to display a warning and consent banner when an administrator attempts to establish an interactive session over the CLI (local or remote) or remote web UI. The TOE also enforces a configurable inactivity timeout for remote administrative sessions.

4.2.7 Trusted Path/Channels

The TOE uses TLS to provide a trusted communication channel between itself and remote servers. The trusted channels utilize X.509 certificates to perform mutual authentication. The TOE initiates the TLS trusted channel with the remote servers.

[1] RSA key generation 4096-bit is vendor affirmed

The TOE uses HTTPS/TLS and SSH to provide a trusted path between itself and remote administrative users. The TOE does not implement any additional methods of remote administration. The remote administrative users are responsible for initiating the trusted path when they wish to communicate with the TOE.

4.2.8 Unevaluated Functionality

The nature of the physical network connection is considered outside the scope of the TOE, as the available network elements (IP switches, IP routers, etc.) which may be used in establishing that link are site-specific. Evertz stipulates that any connection must meet organizationally specific security requirements for the location(s) where the equipment is deployed.

The purpose of the MAGNUM control system is to control a variety of video equipment, including:

- Analog Video Routing Switches
- Digital Video Routing Switches (SDI)
- Digital Video Routing Switches (ASI)
- Digital Video Routing Switches (IP)
- Video Tally Switches
- KVM Routing Switches
- Audio Routing Switches
- Video Master Control Systems
- Video Branding Systems
- Multiviewers
- Video Transport Systems

These will be referred to as “video switches.” These are outside the scope of the TOE.

4.2.9 Excluded Functionality

The TOE includes the following functionality that may not be enabled or used in in the CC evaluated configuration:

- External Authentication Servers for administrator authentication
- SNMP traps

4.3 TOE Documentation

The table below lists the TOE guidance documentation. CC1 and CC2 are delivered via hardcopy to customers with delivery of the TOE. CC3 and ST are provided in .pdf form on the NIAP portal.

Reference	Title	Version	Date
[CC1]	MAGNUM User Manual	1.3	August 2014
[CC2]	MAGNUM Management and Control of Evertz IP Switch Fabrics and Gateways User Manual	0.1	November 2014
[CC3]	MAGNUM Security Administration Manual	26	December 20, 2019
[ST]	Evertz MAGNUM-HW-C-CC Security Target	2.2	December 20, 2019

Table 3 TOE Guidance Documents

4.4 Other References

- collaborative Protection Profile for Network Devices, Version 2.1 [NDcPP]

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

ID	Assumption
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of network devices (e.g, firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trusted source (aka 'root store', 'trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

ID	Threat
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the network device by nefarious means such as masquerading as an administrator to the device, masquerading as the device to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could

	be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

5.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the collaborative Protection Profile for Network Devices, v2.1 (CPP_ND_V2.1).
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- MAGNUM-HW-C-CC Security Target, v2.2, December 20, 2019
- MAGNUM Security Administration Manual, Revision 26, December 20, 2019

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

MAGNUM is a device/component management application specifically designed to operate broadcast and enterprise video switching/routing equipment. Typically, such video equipment is deployed either in an extended series of point-to-point, non-Ethernet connections (such as optical fiber, Serial Digital Interface (SDI), High Density Multimedia Interface (HDMI), HDBaseT, or similar video-specific interfaces) or via an integrated, Ethernet-based switch fabric such as Evertz's IPX product.

MAGNUM does not have the ability to route multimedia stream data and operates exclusively via OOBM. MAGNUM issues operational commands to production video equipment and serves as the primary interface for production devices to report to external services, such as logging tools.

MAGNUM may lie within the same production network as the video equipment or it may be on an isolated network. In the case of non-Ethernet connectivity for the video system, MAGNUM may be located on a standard production network at the discretion of the site/mission owner.

It is not necessary for MAGNUM to be located on an enterprise OOBM network, although sites may choose to do so.

The TOE consists of the MAGNUM-HW-C-CC hardware, running MAGNUM firmware version 19.10.1. Evertz MAGNUM software is a Linux-based application that can be provided on many computing platforms, including Evertz-manufactured control panels. This TOE requires that MAGNUM software be deployed on a dedicated, custom-built Evertz-owned platform (model MAGNUM-HW-C-CC); collectively, this product is known as MAGNUM-HW-C-CC. The MAGNUM-HW-C-CC features an embedded Operating System (OS) on an Intel® Xeon® D-1541 processor and includes the following interfaces:

- 2 x 1 Gigabit Ethernet External Traffic Port
- 2 x RJ45 ports
- 1 x RJ45 dedicated IPMI LAN port
- 2 x USB ports (USB 3.0 connectors)
- VGA Output
- Dual power supply

For local console access a standard video display would be connected via the VGA output and a keyboard would be connected via USB.

The MAGNUM-HW-C-CC device has three components: the MAGNUM software package, an embedded customized Linux distribution, and an Evertz customized hardware platform.

The TOE's operational environment must provide the following services to support the secure operation of the TOE:

Component	Required	Usage/Purpose Description for TOE performance
Syslog server	Yes	• Conformant with RFC 5424 (Syslog Protocol) • Supporting Syslog over TLS (RFC 5425) • Acting as a TLSv1.2 server • Supporting Client Certificate authentication

Component	Required	Usage/Purpose Description for TOE performance
		• Supporting at least one of the following cipher suites: o TLS_RSA_WITH_AES_128_CBC_SHA o TLS_RSA_WITH_AES_256_CBC_SHA o TLS_RSA_WITH_AES_128_CBC_SHA256 o TLS_RSA_WITH_AES_256_CBC_SHA256 o TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 o TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Management workstation with web browser	Yes	• Supported browser: Chrome or Safari • Supporting TLSv1.2 • Supporting Client Certificate authentication • Supporting at least one of the following ciphersuites: o TLS_RSA_WITH_AES_128_CBC_SHA o TLS_RSA_WITH_AES_256_CBC_SHA o TLS_RSA_WITH_AES_128_CBC_SHA256 o TLS_RSA_WITH_AES_256_CBC_SHA256 o TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 o TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
CRL Server	Yes	• Conformant with RFC 5280
DNS Sever	Yes	• Conformant with RFC 1035

7.2 Excluded Functionality

The TOE includes the following functionality that may not be enabled or used in in the CC evaluated configuration:

- External Authentication Servers for administrator authentication
- SNMP traps

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for MAGNUM-HW-C-CC, which is not publicly available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the collaborative Protection Profile for Network Devices v2.1 (CPP_ND_V2.1). The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the MAGNUM-HW-C-CC to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the MAGNUM-HW-C-CC that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the collaborative Protection Profile for Network Devices v2.1 (CPP_ND_V2.1).

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices v2.1 (CPP_ND_V2.1) related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to

securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the collaborative Protection Profile for Network Devices v2.1 (CPP_ND_V2.1) related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the collaborative Protection Profile for Network Devices v2.1 (CPP_ND_V2.1) and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the collaborative Protection Profile for Network Devices v2.1 (CPP_ND_V2.1), and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the collaborative Protection Profile for Network Devices v2.1 (CPP_ND_V2.1), and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the collaborative Protection Profile for Network Devices v2.1 (CPP_ND_V2.1), and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the device(s). The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the devices, to include software that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

Consumers employing the devices must follow the configuration instructions provided in the Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.

It is also recommended that consumers deploy these devices as recommended by the vendor (for example, the vendor recommends these devices be deployed in a closed network).

11 Annexes

Not applicable.

12 Security Target

Please see Section 6

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.