National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

MAGNUM-SC-CC2

Report Number: CCEVS-VR-VID11639-2025

Dated: December 18, 2025

Version: 1.0

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

Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort George G. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Jenn Dotson

Sheldon Durrant

Lisa Mitchell

Linda Morrison

Lori Sarem

The MITRE Corporation

LaChiah Fugh

Matthew Downey

National Information Assurance Partnership

Common Criteria Testing Laboratory

Rupendra Kadtan

Fathi Nasraoui

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-SC-CC2 V24.11.8** 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 **December 2025**. 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 of the below listed PPs.

- *Collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E].
- *Functional Package for SSH*, Version 1.0, 14 May 2021 [PKG_SSH_v1.0].

The TOE identified in this VR 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 Protection Profile (PP). This VR 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 ETR 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 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 ETR 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 PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (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 IT 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 Compliant 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-SC-CC2 V24.11.8
Protection Profile	• *Collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E] • *Functional Package for SSH*, Version 1.0, 14 May 2021 [PKG_SSH_v1.0]
Security Target	*MAGNUM-SC-CC2 Security Target*, version 1.0
Evaluation Technical Report	*Evaluation Technical Report for MAGNUM-SC-CC2*, Version 1.3
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor and Developer	Evertz Microsystems Ltd
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Jenn Dotson, Sheldon Durrant, Lisa Mitchell, Linda Morrison, Lori Sarem (MITRE) LaChiah Fugh, Matt Downey (NIAP)

3 Architectural Information

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-SC-CC2 which includes the MAGNUM-SC-CC2 (1 RU) with an AMD EPYC 7313P (16C/32T) in a Gigabyte E152-ZE1, running MAGNUM-OS firmware v24.11.8. The MAGNUM-OS firmware is based on Ubuntu version 24.04 LTS (Noble). The MAGNUM-OS serves as the primary user and network interface device for the MAGNUM control application.

Evertz MAGNUM software (v24.11.8) is a custom-developed application written primarily in python. MAGNUM-SC-CC2 operates as a combination of an application layer and as part of the integrated Linux platform stack, using a customized Ubuntu operating system. The TOE version of MAGNUM (MAGNUM-SC-CC2) is only operable on Evertz provided platforms and hardware.

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.

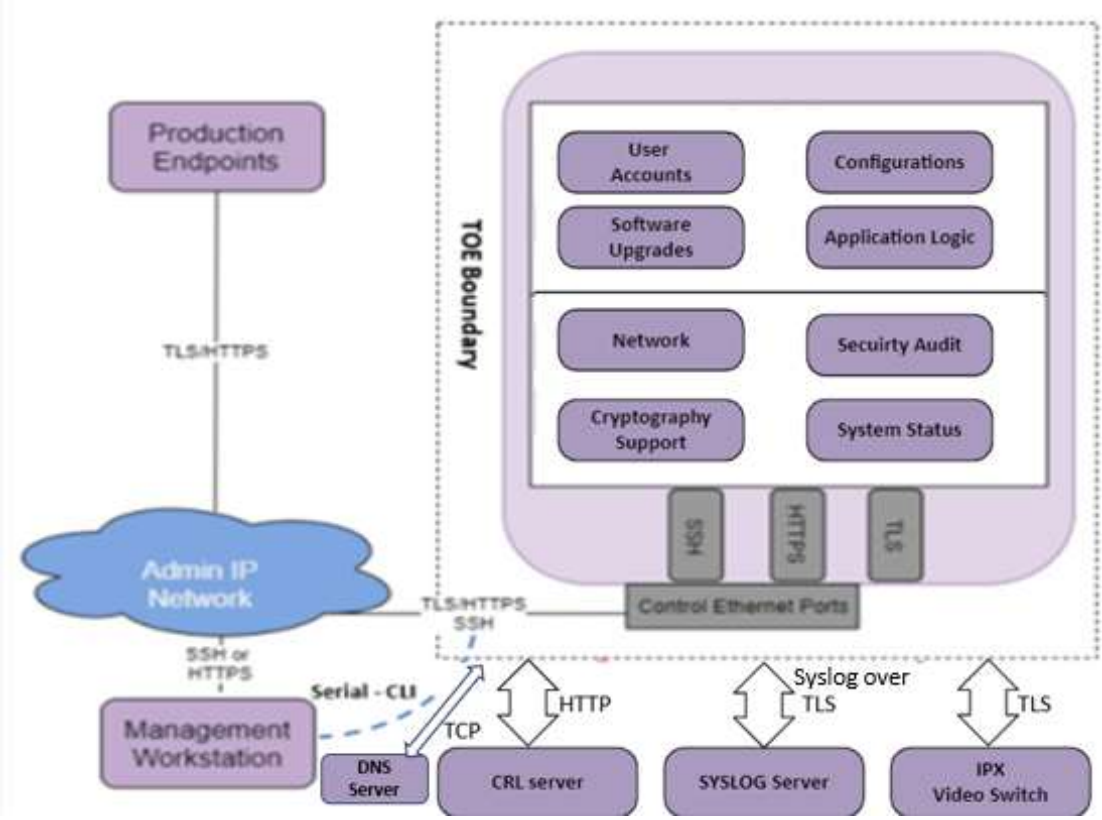

Figure 1 – Representative TOE Deployment

The physical boundaries of the TOE are outlined in Figure 1. The media and video components of the IT environment are NOT part of the TOE physical boundary. The TOE is shipped to the customer via commercial courier.

The IT Testing Environment Components used to test the TOE are shown in Table 2 below:

Table 2: IT Testing Environment Components

Component	Required	Purpose/Description

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
		• Supporting at least one of the following cipher suites:
		  ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
		  ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

IPX Video Switch	Yes	• Provides switching of video signals • Acting as a TLSv1.2 server • Supporting Client Certificate authentication • Supporting at least one of the following cipher suites: ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Component	Required	Purpose/Description
		○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Management workstation with web browser	Yes	• Supported browser: Chrome or Safari • Supporting TLSv1.2 • Supporting at least one of the following ciphersuites: ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Management workstation with remote CLI	Yes	• Supported SSH version: SSHv2 • Conformant with RFCs 4251-4254, 5647, 5656, 8308 and 8332.
Local Management Workstation	Yes	• Computer with terminal emulation software to access the console interface (CLI)
CRL Server	Yes	• Conformant with RFC 5280 • Provides a list of revoked certificates. • TOE uses the CRL server to check the revocation status of a server's presented certificate. • Communication between the TOE and the CRL server occurs over HTTP.
DNS Server	Yes	• Conformant with RFC 1035. • Communication between the TOE and the DNS server occurs over TCP.

4 Security Policy

The TOE provides the security functions required by the Collaborative Protection Profile for Network Devices, hereafter referred to as NDcPP v3.0e or NDcPP and Functional Package for SSH, Version 1.0, hereafter referred to as PKG_SSH_v1.0.

This section summarizes the security functionality of the TOE:

1.) Security audit
2.) Cryptographic support
3.) Identification and authentication
4.) Security management
5.) Protection of the TSF
6.) TOE access
7.) Trusted path/channels

4.1 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 access to the TSF using administrator accounts 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 Cryptographic Support

The TOE includes an OpenSSL library (openssl_3.0.13-0ubuntu3.5, openssl_fips version 3.0.9et2 and linux-image-generic_6.8.0.71) 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:

Table 3: TOE Cryptographic Protocols

Cryptographic Protocol	Use within the TOE
TLS (client)	**Secure connection to syslog and IPX video switches** **FCS_TLSC_EXT.1, FCS_TLSC_EXT.2**

Cryptographic Protocol	Use within the TOE
HTTPS/TLS (server)	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_COP.1.1/DataEncryption ,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, FCS_SSHS_EXT.1
HMAC	Provides keyed hashing services in support of TLS. FCS_COP.1/KeyedHash, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1, FCS_SSHS_EXT.1
EC-DH	Provides key establishment for TLS. FCS_CKM.2, FCS_TLSC_EXT.2, FCS_TLSS_EXT.1, FCS_SSHS_EXT.1
ECDSA	Used to generate EC-DH components for key establishment for TLS. FCS_CKM.1, FCS_CKM.2, FCS_TLSS_EXT.1, FCS_SSHS_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, FCS_SSHS_EXT.1

4.3 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.

4.4 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.

4.5 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.

4.6 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.

4.7 Trusted Path/Channels

The TOE uses Syslog over TLS to provide a trusted communication channel between itself and remote audit server and IP Video switch. The trusted channels utilize X.509 certificates to perform mutual authentication. The TOE initiates the TLS trusted channel with the remote server.

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.

5 Assumptions & Clarification of Scope

5.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- Collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E]
- Functional Package for SSH, Version 1.0, 14 May 2021 [PKG_SSH_v1.0]

That information has not been reproduced here and the CPP_ND_V3.0E/PKG_SSH_v1.0 should be consulted if there is interest in that material.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the CPP_ND_V3.0E/PKG_SSH_v1.0 as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

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 CPP_ND_V3.0E/PKG_SSH_v1.0.
- Consistent with the expectations of the PP, 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.
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- Apart from the Admin Guide, additional customer documentation for the specific models was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.
- 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-SS-CC2 Supplemental Administrative Guidance for Common Criteria*, Version 0.7.

Any additional customer documentation provided with the product, or that is available online was not included in the scope of the evaluation and therefore should not be relied upon when configuring or operating the device as evaluated.

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

7 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in ETR for **MAGNUM-SC-CC2 V24.11.8**, which is not publicly available. The AAR provides an overview of testing and the prescribed assurance activities.

7.1 Developer Testing

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

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according to the vendor-provided guidance documentation and ran the tests specified in the below claimed PPs.

- Collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E]
- Functional Package for SSH, Version 1.0, 14 May 2021 [PKG_SSH_v1.0].

The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

8 TOE Evaluated Configuration

8.1 Evaluated Configuration

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

The following environmental components are required to operate the TOE in the evaluated configuration:

Table 4: Required Environmental Components

Component	Purpose/Description
Syslog server	• Conformant with RFC 5424 (Syslog Protocol) • Supporting Syslog over TLS (RFC 5425) • Acting as a TLSv1.2 server • Supporting Client Certificate authentication • Supporting at least one of the following cipher suites: ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
IPX Video Switch	• Provides switching of video signals • Acting as a TLSv1.2 server • Supporting Client Certificate authentication • Supporting at least one of the following cipher suites: ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Management workstation with web browser	• Supported browser: Chrome or Safari • Supporting TLSv1.2 • Supporting at least one of the following ciphersuites: ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
Management workstation with remote CLI	• Supported SSH version: SSHv2 • Conformant with RFCs 4251-4254, 5647, 5656, 8308 and 8332.
Local Management Workstation	• Computer with terminal emulation software to access the console interface (CLI)
CRL Server	• Conformant with RFC 5280. • Provides a list of revoked certificates.

Component	Purpose/Description
	• TOE uses the CRL server to check the revocation status of a server's presented certificate. • Communication between the TOE and the CRL server occurs over HTTP.
DNS Server	• Conformant with RFC 1035. • Communication between the TOE and the DNS server occurs over TCP.

8.2 Excluded Functionality

The following product functionality is not included in the CC evaluation:

- External Authentication Servers for administrator authentication
- SNMP traps
- Media streaming systems and devices controller feature

The MAGNUM is a software module that unifies control and interfacing to Evertz and 3rd party media steaming devices. As a unified controller, the MAGNUM supports the following functionalities that are outside of the scope of this evaluation:

- 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.
- 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-SC-CC2 device serves as the primary operational and administrative management interface to the closed multicast switching environment.
- MAGNUM provides Out-of-Band Management (OOBM) of Evertz IPX, EXE, and other 3rd party devices. To perform primary operational and administrative management functions on the closed multicast switching environment, Security Administrators may access MAGNUM software via direct connection using a terminal session. Security Administrators may also access MAGNUM via a dedicated management workstation operating over an OOBM network to perform these OOB management functions. In addition to Security Administrators, general users may also access the MAGNUM software via a dedicated management workstation over an OOBM network.

Note: Sites may close this OOBM network or may operate MAGNUM within an existing OOBM, if the topology is compliant with the security parameters listed below.

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 ETR. The reader of this document can assume that all 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. (5) and CEM version 3.1 Rev. (5). The Evaluation team determined the **MAGNUM-SC-CC2 V24.11.8** to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the Evaluation team performed the Assurance Activities specified in the CPP_ND_V3.0E/PKG_SSH_v1.0.

9.1 Evaluation of Security Target (ASE)

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-SC-CC2 V24.11.8** that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the Evaluation team performed an assessment of the Assurance Activities specified in the CPP_ND_V3.0E/PKG_SSH_v1.0 .

The Validation team 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 (ADV)

The evaluation team applied each 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 ST's TOE Summary Specification (TSS) and the Guidance documents. Additionally, the Evaluation team performed the Assurance Activities specified in the CPP_ND_V3.0E/PKG_SSH_v1.0 related to the examination of the information contained in the TSS.

The Validation team 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 (AGD)

The Evaluation team applied each 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 Evaluation team performed the Assurance Activities specified in the CPP_ND_V3.0E/PKG_SSH_v1.0 related to the examination of the information contained in the operational guidance documents.

The Validation team 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 (ALC)

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was identified.

The Validation team 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 (ATE)

The Evaluation team applied each ATE CEM work unit. The Evaluation team ran the set of tests specified by the Assurance Activities in the CPP_ND_V3.0E/PKG_SSH_v1.0 and recorded the results in a Test Report, summarized in the ETR and AAR.

The Validation team 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 CPP_ND_V3.0E/PKG_SSH_v1.0, and that the conclusion reached by the Evaluation team was justified.

9.6 Vulnerability Assessment Activity

The Evaluation team applied each 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 Evaluation team searched the National Vulnerability Database (https://nvd.nist.gov/view/vuln.search), MITRE CVE Database (http://cve.mitre.org/cve) CVE Details (https://www.cvedetails.com/vulnerability-search.php), and Evertz database (https://evertz.com/) on March 12, June 4, September 10th, and November 18, 2025 for search terms including the vendor name, product name, and key platform features and libraries leveraged by the product. A full list of the search terms can be found in Section 6.4.1.2 of the

AAR.

The Validation team 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 CPP_ND_V3.0E/PKG_SSH_v1.0, 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 followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The Validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the *MAGNUM-SS-CC2 Supplemental Administrative Guidance for Common Criteria*, Version 0.7. As stated in the Clarification of Scope, the evaluated functionality is scoped exclusively to the security functional requirements specified in the ST, and the only evaluated functionality was that which was described by the SFRs claimed in the ST. All other functionality provided by the TOE needs to be assessed separately and no further conclusions can be drawn about its effectiveness.

Consumers employing the TOE 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 important to note the excluded functionality listed in Section 8.2 and follow the configuration instructions to ensure that this functionality is disabled.

Evaluation activities are strictly bound by the assurance activities described in the CPP_ND_V3.0E/PKG_SSH_v1.0 and accompanying Supporting Documents. Consumers and integrators of this TOE are advised to understand the inherent limitations of these activities and take additional measures as needed to ensure proper TOE behavior when integrated into an operational environment.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as: *MAGNUM-SC-CC2 Security Target*, Version 1.0.

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.
5. *Collaborative Protection Profile for Network Devices*, Version 3.0e, 06 December 2023 [CPP_ND_V3.0E].
6. *Functional Package for SSH*, Version 1.0, 14 May 2021 [PKG_SSH_v1.0].
7. *MAGNUM-SC-CC2 Security Target*, Version 1.0.
8. *Assurance Activity Report for MAGNUM-SC-CC2*, Version 1.4.
9. *Evaluation Technical Report for MAGNUM-SC-CC2*, version 1.3.
10. *Test Plan Report for Magnum-SC-CC2*, version 1.2.
11. *MAGNUM-SC-CC2 Supplemental Administrative Guidance for Common Criteria*, Version 0.7.
12. *Vulnerability Assessment for Evertz Microsystems: MAGNUM-SC-CC2 v24.11.8*, Version 1.7.