National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Evertz Magnum, Version 1.0

Report Number:	**CCEVS-VR-10828-2017**
Dated:	**12/8/2017**
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

Paul Bicknell

Sheldon Durrant

Linda Morrison

The MITRE Corporation

Common Criteria Testing Laboratory

Pascal Patin

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 Evertz Magnum 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 2017. 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 Network Device collaborative Protection Profile v1.0 (NDcPP).

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. 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 4), as interpreted by the Assurance Activities contained in the NDcPP. 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, reviewed the individual work units documented in the Assurance Activities Report (AAR), and also examined the Evaluation Technical Report (ETR). 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 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 Protection Profile 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	Evertz Magnum-SC-CC
Protection Profile	Network Device collaborative Protection Profile v1.0
Security Target	Evertz MAGNUM-SC-CC PPAS v2.6 Security Target
Evaluation Technical Report	Evertz Magnum ETR 1.0
CC Version	Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Evertz Microsystems Ltd.
Developer	Evertz Microsystems Ltd.
Common Criteria Testing Lab (CCTL)	Acumen Security Montgomery Village, MD
CCEVS Validators	Paul Bicknell Sheldon Durrant Linda Morrison The MITRE Corporation

3 Architectural Information

The MAGNUM-SC-CC hardware device is the Evertz MAGNUM-SC-CC running MAGNUM software. The MAGNUM-SC-CC serves as the primary user and network interface device for the MAGNUM control application.

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.

Traditional packet-based networks do not support the extremely high standards for signal integrity and fault tolerance required for broadcast video. Evertz's solution to this problem has been to develop a packet-based switching fabric from a video perspective, rather than rely on traditional packet-based network architecture. Since video by nature has a unidirectional flow, and also since it is normal for multiple copies of a single incoming video stream to be sent to multiple output destinations, Evertz focuses exclusively on multicast IP addressing. Unicast is not feasible for streaming video in an enterprise production environment.

Multicast switching can be challenging, especially for non-automated systems. Momentary delays and signal loss are common in these networks but are unacceptable in broadcast environments. Evertz has approached the problem from a video perspective. MAGNUM-SC-CC controls all Evertz multicast group definitions using a proprietary multicast protocol. MAGNUM compiles and delivers these commands within the context of traditional "vertical interval" switching architectures for legacy broadcast routing architectures, so as to route data seamlessly between program streams in a manner sufficient to meet broadcast video standards for signal availability and integrity.

The equipment to prepare video for IP transport, or to convert it into other video formats, is outside the scope of the 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 the TOE.

4 Security Policy

The NDcPP-compliant TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

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

These features are described in more detail in the subsections below.

4.1 Security Audit

The TOE's Audit security function supports audit record generation and review. The TOE provides date and time information that is used in audit timestamps. Very broadly, the Audit events generated by the TOE include:

- Establishment of a Trusted Path or Channel Session
- Failure to Establish a Trusted Path or Channel Session
- Termination of a Trusted Path or Channel Session
- Failure of Trusted Channel Functions
- Identification and Authentication
- Unsuccessful attempt to validate a certificate
- Any update attempt
- Result of the update attempt
- Management of TSF data
- Changes to Time

The TOE can store the generated audit data on itself and it can be configured to send syslog events to a syslog server, using a TLS protected collection method. Logs are classified into various predefined categories. The logging categories help describe the content of the messages that they contain. Access to the logs is restricted to only Security Administrators, who have no access to edit them, only to copy or delete (clear) them. Audit records are also protected from unauthorized modifications and deletions.

The logs can be viewed by using a drop-down menu feature. The logs record the time, host name, facility, application and "message" (i.e., the log details). New audit records are dropped when the allocated space for these records reaches the threshold, which is why the use of a syslog server is important.

4.2 Cryptographic Support

The TOE provides cryptography support for secure communications and protection of information. The cryptographic services provided by the TOE include: symmetric encryption and decryption using AES; cryptographic hashing and software integrity testing using SHS; keyed hashing services using HMAC-SHA; random-bit generation using DRBG; cryptographic key establishment using RSA-based key establishment schemes; digital signature using RSA; key agreement using CVL-KAS-FFC. The TOE implements secure protocols TLS (Server and Client) and TLS/HTTPS (Server). The algorithm certificate references are listed in the table below.

Algorithm	Description	Mode Supported	CAVP Cert. #
AES	Used for symmetric encryption/decryption FCS_TLSC_EXT.2 FCS_TLSS_EXT.1 FCS_HTTPS_EXT.1 FCS_COP.1(1)	CBC (128 and 256 bits) and GCM (128 and 256 bits)	4651
SHS (SHA-1, SHA-256, SHA-384 and SHA-512)	Cryptographic hashing services and software integrity test FCS_TLSC_EXT.2 FCS_TLSS_EXT.1 FCS_HTTPS_EXT.1 FCS_COP.1(1) FCS_COP.1(3)	Byte Oriented	3810
HMAC (HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-384)	Keyed hashing services FCS_TLSC_EXT.2 FCS_TLSS_EXT.1 FCS_HTTPS_EXT.1 FCS_COP.1(1) FCS_COP.1(4)	Byte Oriented	3079
DRBG	Deterministic random bit generation services in accordance with NIST SP 800-90A Rev 1 FCS_TLSC_EXT.2 FCS_TLSS_EXT.1 FCS_HTTPS_EXT.1 FCS_RBG_EXT.1	CTR_DRBG (AES 256)	1569
RSA	Signature Verification and key transport	FIPS PUB 186-4 Key Generation (2048-bit key)	2537

	FCS_TLSC_EXT.2 FCS_TLSS_EXT.1 FCS_HTTPS_EXT.1 FCS_CKM.1 FCS_CKM.2 FCS_COP.1(2)		

Table 1. CAVP Certification References

4.3 Identification and Authorization

All Administrators wanting to use TOE services are identified and authenticated prior to being allowed access to any of the services other than the display of the warning banner. Once an Administrator attempts to access the management functionality of the TOE, the TOE prompts the Administrator for a user name and password for password-based authentication. The identification and authentication credentials are confirmed against a local user database. Only after the Administrator presents the correct identification and authentication credentials will access to the TOE functionality be granted. The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS/HTTPS connections.

The TOE provides the capability to set password minimum length rules. This is to ensure the use of strong passwords in attempts to protect against brute force attacks. The TOE also accepts passwords composed of a variety of characters to support complex password composition. During authentication, no indication is given of the characters composing the password.

4.4 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure session or a local console connection. The TOE provides the ability to perform the following actions:

- Administer the TOE locally and remotely
- Configure the access banner
- Configure the cryptographic services
- Update the TOE and verify the updates using digital signature capability prior to installing those updates
- Specify the time limits of session inactivity

All of these management functions are restricted to an Administrator, which covers all administrator roles. Administrators are individuals who manage specific type of administrative tasks.

Primary management is done using the local console or remotely via HTTPS. This provides a network administration console from which one can manage various identity services. These services include authentication, authorization and reporting. All of these services use a menu-driven navigation system.

4.5 Protection of the TSF

The TOE will terminate inactive sessions after an Administrator-configurable time period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. The TOE provides protection of TSF data (authentication data and cryptographic keys). In addition, the TOE internally maintains the date and time. This date and time is used as the time stamp that is applied to TOE generated audit records. This time can be set by an Administrator using the "Date" and "Time" selections from the System Configuration menu, or can be set to follow an external NTP server. The TOE also ensures firmware updates are from a reliable source. Finally, the TOE performs testing to verify correct operation.

In order for updates to be installed on the TOE, an administrator initiates the process from the web interface. Magnum automatically uses the digital signature mechanism to confirm the integrity of the product before installing the update.

4.6 TOE Access

Aside from the automatic Administrator session termination due to inactivity describes above, the TOE also allows Administrators to terminate their own interactive session. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

Regardless of the type of connection the TOE will display an Administrator-specified banner on the web browser management interface prior to allowing any administrative access to the TOE.

4.7 Trusted Paths/Channels

Magnum allows the establishment of a trusted path between a itself and various video control switches (such as Evertz' IPX); it can also link to an additional Magnum (for primary / backup control arrangements). The TOE also establishes a secure connection for sending syslog data to a syslog server using TLS and other external authentication stores using TLS-protected communications.

5 Assumptions, Threats & 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 1.0, 27 February 2015 (NDcPP)

That information has not been reproduced here and the NDcPP should be consulted if there is interest in that material.

5.2 Threats

The Security Problem Definition, including the threats, may also be found in the NDcPP. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

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 NDcPP. All NIAP Technical Decisions related to the protection profile security functional requirements were considered and applied as necessary.
- This evaluation covers only the specific device models and software as identified in Security Target, and not any earlier or later versions released or in process.
- 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 PP. 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:

- Evertz MAGNUM-SC-CC PPAS v2.6 Security Target
- Magnum SDVN Security Administration Manual, Revision 19

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The evaluated configuration of the TOE is clearly identified in the Security Target.

7.2 Excluded Functionality

The ST describes “Non-Scope Elements”, such as video switches, that are outside of were not considered during the evaluation.

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 Evertz Magnum, which is not publically 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 NDcPP. The Independent Testing activity is documented in the Assurance Activities Report, which is publically 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 Evertz Magnum 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 Evertz Magnum 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 NDcPP.

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 NDcPP 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 NDcPP 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 NDcPP 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 NDcPP, 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 NDcPP, 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 NDcPP, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validators suggest that consumers pay particular attention to the evaluated configuration of the device(s). Those employing the devices must follow the configuration instructions provided in the Users Guidance documentation listed above to ensure the evaluated configuration is established and maintained.

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, including the Excluded Functionality discussed above, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

The evaluated version of the products utilizes *MAGNUM OpenSSL Cryptographic Module, Version 1.16.0* crypto software and the *Intel Xeon CPU D-1541* processor and no earlier or later versions were evaluated and therefore cannot be considered as compliant.

The TOE stores a limited amount of audit records in its internal persistent storage. It is recommended that the administrator configure the TOE to export audit logs to a remote audit storage server.

11 Annexes

Not applicable.

12 Security Target

Evertz MAGNUM-SC-CC PPAS v2.6 Security Target

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 4.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.