National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

Bivio Networks, Inc.

Bivio 6310-NC

Report Number: CCEVS-VR-VID10873_2018
Dated: April 25, 2018
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 Panel

Patrick Mallett, PhD.
MITRE Corporation, McLean, Va.
Kenneth Stutterheim
The Aerospace Corporation,
Columbia, Md.

Common Criteria Testing Laboratory

Michael C. Baron
Ryan Day
UL Verification Services Inc.
San Luis Obispo, CA

Table of Contents

1 Executive Summary

This report documents the NIAP validators' assessment of the CCEVS evaluation of the Bivio 6310-NC.

This report is intended to assist the end-user of this product with determining the suitability of this IT product in their environment. End-users should review both the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated.

The TOE is classified as a Network Device (a generic infrastructure device that can be connected to a network).

The Bivio 6310-NC device can be used to run a variety of applications for processing network data. There are many such applications, both commercial and open source. It is out of scope for the certification process to include those applications for evaluation, however a standard application factory-installed to all Bivio 6310-NC devices as part of the base BiviOS has been provided.

TOE's are identified with a part number in the format

- B6310-NC-C(1,2,3,5,6)M(1,2,3,4,5)D(1,2,3,4,5,6)N(1,2,3,4)
    - This chassis is the "standard" product chassis.
- B6310R-NC-C(5,6)M(1,2,3)D(1,2,3,4,5,6)N(1,2,4)
    - This chassis is a shorter, ruggedized chassis
- PacStar 451
    - This chassis does not have configuration options, and will always use the "C4" processor specification (defined below)

The naming conventions specified above reference the following hardware:

Table 1: Available TOE Hardware Configuration	
Part Number	Processor
Options with C1	Dual Intel Xeon Gold 6148, 2.4 GHz w/ 27Mb Cache
Options with C2	Dual Intel Xeon Platinum 8180, 2.5 GHz w/ 38Mb Cache
Options with C3	Dual Intel Xeon Silver 4110, 2.1 GHz w/ 11Mb Cache
Options with C4	Intel Xeon E3-1515Mv5, 2.8 GHz w/ 8Mb Cache
Options with C5	Dual Intel Xeon Gold 6138, 2.0 GHz w/27Mb Cache
Options with C6	Dual Intel Xeon Gold 6152, 2.1 GHz w/30Mb Cache
Part Number	Installed RAM

Options with M1	256GB DDR4-2666 memory
Options with M2	512GB DDR4-2666 memory
Options with M3	384GB DDR4-2666 memory
Options with M4	768GB DDR4-2666 memory
Options with M5	1536GB DDR4-2666 memory
Part Number	Installed Storage
Options with D1	2x 1TB SSD storage
Options with D2	2x 2TB SSD storage
Options with D3	4x 2TB SSD storage
Options with D4	8x 2TB SSD storage
Options with D5	4x 3.8TB SSD storage
Options with D6	8x 3.8TB SSD storage
Part Number	Installed NIC Interfaces
Options with N1	2x 10GbE Fiber interfaces and 4x 1GbE Copper interfaces
Options with N2	4x 10GbE Fiber interfaces and 4x 1GbE Copper interfaces
Options with N3	6x 10GbE Fiber interfaces and 2x 1GbE Copper interfaces
Options with N4	4x 10GbE Fiber interfaces and 2x 1GbE Copper interfaces

Note: All CPUs utilized in the platforms of the TOE are 'Intel Xeon Skylake' processors.

Running the following software:

- BiviOS 8.3.1 (Build 201704241036)

The guidance documentation is also part of the TOE. A list of the guidance documents can be found in Table 12 of the Security Target.

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

- Local Console
- Syslog Server
- An SSHv2 Client
- A TLSv1.2 client

This table identifies components that must be present in the Operational Environment to support the operation of the TOE.

Component	Description
Local Console	• A local console with an RS-232 port for use with the Bivio provided console cable.
Syslog Server (Remote Audit Server)	• Syslog server conformant to RFC 5424 (Syslog over TCP capable of receiving an SSH tunnel from the TOE.
SSHv2 Client (Remote Administrative Access)	• Administrators will need an SSHv2 Client conformant to RFCs 4251, 4252, 4253, 4254, and 6668. o The SSHv2 client must be capable of supporting AES128-CBC and AES256-CBC encryption algorithms, using HMAC-SHA2-256 or HMAC-SHA2-512 integrity algorithms, and performing key exchange using Diffie-Hellman Group14-SHA1. o To perform public-key authentication to the TOE, the SSHv2 client must be capable of supporting SSH-RSA.
TLS Client (Remote Administrative Access)	• The TOE provides TLS protected server capability, which requires a TLSv1.2 client capable of negotiating one of the following ciphersuites: o TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 o TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

Table 2: Operational Environment Components

2 Identification of the TOE

Table 3 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 organizations and individuals participating in the evaluation.

Evaluation Scheme	United States Common Criteria Evaluation Validation Scheme
Evaluated Target of Evaluation	Bivio 6310-NC
Protection Profile	collaborative Protection Profile for Network Devices, Version 1.0, dated February 27, 2015 [NDcPP]
Security Target	Bivio 6310-NC Security Target Version 1.1, April 20, 2018
Dates of Evaluation	January-April 2018
Conformance Result	Pass
Common Criteria Version	3.1r4
Common Evaluation Methodology (CEM) Version	3.1r4
Evaluation Technical Report (ETR)	18-4135-R-0036 V1.1, April 20, 2018
Sponsor/Developer	Bivio Networks, Inc.
Common Criteria Testing Lab (CCTL)	UL Verification Services Inc.
CCTL Evaluators	Michael C. Baron, Ryan Day
CCEVS Validators	Patrick Mallett PhD., Kenneth Stutterheim

Table 3: Product Identification

3 Interpretations

The Evaluation Team performed an analysis of the international interpretations of the CC and the CEM and determined that none of the International interpretations issued by the Common Criteria Interpretations Management Board (CCIMB) were applicable to this evaluation.

The TOE is also compliant with all international interpretations with effective dates on or before March 15, 2018.

4 Security Policy

This section contains the product features and denotes which are within the logical boundaries of the TOE. The following Security Functions are supported by the TOE:

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

4.1 Audit

- The TOE will audit all events and information defined in Table 7 of the Security Target.
- The TOE will also include the identity of the user that caused the event (if applicable), date and time of the event, type of event, and the outcome of the event.
- The TOE protects storage of audit information from unauthorized deletion.
- The TOE prevents unauthorized modifications to the stored audit records.
- The TOE can transmit audit data to an external IT entity using SSH protocol.

4.2 Cryptographic Operations

The TSF performs the following cryptographic operations:

For TLS:

- AES-128 in CBC mode for data ciphering, using SHA-1 hashing and RSA key exchange. AES-256 in GCM mode for data ciphering, using SHA-384 hashing and ECDHE key exchange.

For SSH:

- AES-128 or AES-256 in CBC mode, HMAC-SHA2-256 or HMAC-SHA2-512 hashing and DH key exchange.
- Public key authentication via SSH-RSA, using HMAC-SHA1 hashing.

The TSF zeroizes all plaintext secret and private cryptographic keys and CSPs once they are no longer required.

4.3 Identification and Authentication

- The TSF supports passwords consisting of alphanumeric and special characters. The TSF also allows administrators to set a minimum password length and support passwords with 15 characters or more.
- The TSF requires all administrative-users to authenticate before allowing the user to perform any actions other than:

- Viewing the warning banner
- Responding to ICMP echo requests
- Responding to ARP requests with ARP replies
- Responding to DNS requests

4.4 Security Management

- The TSF stores and protects the following data:
  - Syslog data, user account data, and local authentication data (such as administrator passwords).
  - Cryptographic keys, including pre-shared keys, symmetric keys, and private keys.
- There are two classes of users on the TOE:
  - First, the Admin user. The Admin user has full control over the TOE and can create other users (for instance, multiple administrative users) and control their level of access to the TOE.
  - Second, any administrator-created non-administrative user accounts. This would be a highly unusual configuration, as in most cases there is no reason to create a non-administrator account for the TOE. The TOE does not offer any functionality that requires users to authenticate other than to perform administration of the TOE.
- Management of the TSF:
  - The administrator can perform manual updates, determine the behavior of or modify the behavior of the handling of audit data, modify the behavior of the TSF, enable or disable services offered by the TOE, determine the behavior of or modify the behavior of audit functionality when local audit storage is full, manage TSF data, modify or delete or generate or import cryptographic keys, configure the access banner, and configure the session inactivity timeout period.
  - The administrator may perform these functions locally or remotely using the trusted path provided by SSH and defined in FTP_TRP.1.

4.5 Protection of the TSF

- The TSF protects TSF data from disclosure when the data is transmitted between different parts of the TOE.
- The TSF prevents the reading of secret and private keys.
- The TOE provides reliable time stamps for itself.
- The TOE runs a suite of self-tests during the initial start-up (upon power on) to demonstrate the correction operation of the TSF.
- The TOE provides a means to verify firmware/software updates to the TOE using a published hash prior to installing those updates.

4.6 TOE Access

- The TOE, for local interactive sessions, will terminate the session after an Authorized Administrator-specified period of session inactivity.

- The TOE terminates a remote interactive session after an Authorized Administrator-configurable period of session inactivity.
- The TOE allows Administrator-initiated termination of the Administrator's own interactive session.
- Before establishing an administrative user session, the TOE can display an Authorized Administrator-specified advisory notice and consent warning message regarding unauthorized use of the TOE.

4.7 Trusted Path/Channels

- The TOE uses SSH to provide a trusted communication channel between itself and all authorized IT entities that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.
- The TOE permits the TSF, or the authorized IT entities, to initiate communication via the trusted channel.
- The TOE uses SSH or TLS to provide a trusted communication path between itself and authorized administrative users that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.
- The TOE permits remote administrators to initiate communication via the trusted path.
- The TOE requires the use of the trusted path for initial administrator authentication and all remote administration actions.

5 TOE Security Environment

5.1 Secure Usage Assumptions

The following assumptions are made about the usage of the TOE:

Table 4: Assumptions

Assumption	Description
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

Table 4: Assumptions	
Assumption	Description
	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 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.
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.

5.2 Threats Countered by the TOE

The TOE is designed to counter the following threats:

Table 5: Threats	
Threat	Description
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., 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,

Table 5: Threats	
Threat	Description
	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 include 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	A component of the network device may fail during start-up or during operations causing a compromise or failure in the security functionality of the network device, leaving the device susceptible to attackers.

5.3 Organizational Security Policies

The TOE enforces the following OSPs:

Table 6: Organizational Security Policies	
OSP	Description
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

5.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. 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 assurance activities specified in the claimed PPs and performed by the evaluation team).
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality

specified in the claimed PP. Any additional security related functional capabilities of the product discussed in supporting documentation were not covered by this evaluation. The following list of services provided by the models is outside the scope of this evaluation:

- The application that is factory-installed to all Bivio 6310-NC devices as part of the base product. The application is not evaluated and provides non-evaluated functionality.
- This evaluation did not specifically search for, nor attempt to exploit, 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.

6 Architectural Information

The TOE is classified as Network Device for Common Criteria purposes.

6.1 Architecture Overview

The TOE consists of hardware and software components.

6.1.1 TOE Hardware

The TOE consists of the following hardware and are identified with a part number in the format:

- B6310-NC-C(1,2,3,5,6)M(1,2,3,4,5)D(1,2,3,4,5,6)N(1,2,3,4)
    - This chassis is the “standard” product chassis
- B6310R-NC-C(5,6)M(1,2,3)D(1,2,3,4,5,6)N(1,2,4)
    - This chassis is a shorter, ruggedized chassis
- PacStar 451
    - This chassis does not have configuration options, and will always use the “C4” processor specification (defined below)

The naming conventions specified above reference the following hardware:

Table 1: Available TOE Hardware Configuration

Part Number	Processor
Options with C1	Dual Intel Xeon Gold 6148, 2.4 GHz w/ 27Mb Cache
Options with C2	Dual Intel Xeon Platinum 8180, 2.5 GHz w/ 38Mb Cache
Options with C3	Dual Intel Xeon Silver 4110, 2.1 GHz w/ 11Mb Cache
Options with C4	Intel Xeon E3-1515Mv5, 2.8 GHz w/ 8Mb Cache
Options with C5	Dual Intel Xeon Gold 6138, 2.0 GHz w/27Mb Cache

Options with C6	Dual Intel Xeon Gold 6152, 2.1 GHz w/30Mb Cache
Part Number	Installed RAM
Options with M1	256GB DDR4-2666 memory
Options with M2	512GB DDR4-2666 memory
Options with M3	384GB DDR4-2666 memory
Options with M4	768GB DDR4-2666 memory
Options with M5	1536GB DDR4-2666 memory
Part Number	Installed Storage
Options with D1	2x 1TB SSD storage
Options with D2	2x 2TB SSD storage
Options with D3	4x 2TB SSD storage
Options with D4	8x 2TB SSD storage
Options with D5	4x 3.8TB SSD storage
Options with D6	8x 3.8TB SSD storage
Part Number	Installed NIC Interfaces
Options with N1	2x 10GbE Fiber interfaces and 4x 1GbE Copper interfaces
Options with N2	4x 10GbE Fiber interfaces and 4x 1GbE Copper interfaces
Options with N3	6x 10GbE Fiber interfaces and 2x 1GbE Copper interfaces
Options with N4	4x 10GbE Fiber interfaces and 2x 1GbE Copper interfaces

Note: All CPUs utilized in the platforms of the TOE are 'Intel Xeon Skylake' processors.

6.1.2 TOE Software

The TOE runs the following software:

- BiviOS 8.3.1 (Build 201704241036)

7 Documentation

This section details the documentation that is (a) delivered to the customer, and (b) was used as evidence for the evaluation of the Bivio 6310-NC TOE. In these tables, the following conventions are used:

- Documentation that is delivered to the customer is shown with **bold** titles.
- Documentation that was used as evidence but is not delivered is shown in a normal

typeface.

- Documentation that is delivered as part of the product but was not used as evaluation is shown with a hashed background.

The guidance documents are provided to the product consumer via download from a web-based customer portal provided by the vendor. These documents apply to the CC Evaluated configuration:

7.1 Design Documentation

Document	Revision	Date
Bivio 6310-NC Lifecycle and Product Labelling Q & A	1.0	February 26, 2018
Bivio 6310-NC Development and Design Assessment Q & A	1.0	February 26, 2018

7.2 Guidance Documentation

Document	Revision	Date
Bivio 6310-NC Common Criteria Administrative Guidance	1.3	March 8, 2018

7.3 Test Documentation

Document	Revision	Date
18-4135-R-0002 Test Report (Evaluation Sensitive)	1.2	April 20, 2018

7.4 Vulnerability Assessment Documentation

Document	Revision	Date
18-4135-R-0002 Test Report (Evaluation Sensitive)	1.2	April 20, 2018

7.5 Security Target

Document	Revision	Date
Bivio 6310-NC Security Target	1.1	April 20, 2018

7.6 Assurance Activity Report

Document	Revision	Date
Assurance Activity Report, VID 10873, 18-4135-R-0004	1.1	April 20, 2018

Any additional customer documentation provided with the product, or that which may be available online was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated.

8 IT Product Testing

This section describes the testing efforts of the Developer and the Evaluation Team.

8.1 Developer Testing

No testing was performed by the developer.

8.2 Evaluation Team Independent Testing

The evaluation team performed the independent testing activities to confirm the TOE operates to the TOE security functional requirements as specified in the ST for a product claiming conformance to the collaborative Protection Profile for Network Devices, Version 1.0, February 27, 2015. The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the NDcPP. The Test Plan described how each test activity was to be performed. The evaluation team executed the tests specified in the Test Plan and documented the results in a proprietary 'Test Document' listed above in Section 7.3. The results of the testing are summarized in the publicly available Assurance Activity Report for this evaluation.

Independent testing was performed at the UL facility in San Luis Obispo, CA. The hardware/software was provided in the same form that customers would receive it. The evaluator installed and configured the TOE in accordance with the vendor provided guidance documentation and performed the testing procedures as described in the Test Documentation.

8.3 Test Tools

- Linux Kali 4.3.0
- Nmap 7.01
- Zenmap 7.01
- Wireshark 2.0.1
- Apache Web Server 2.2.15
- OpenSSH 5.3
- OpenSSL 1.0

- Rsyslog 8.16

8.4 Test Environment

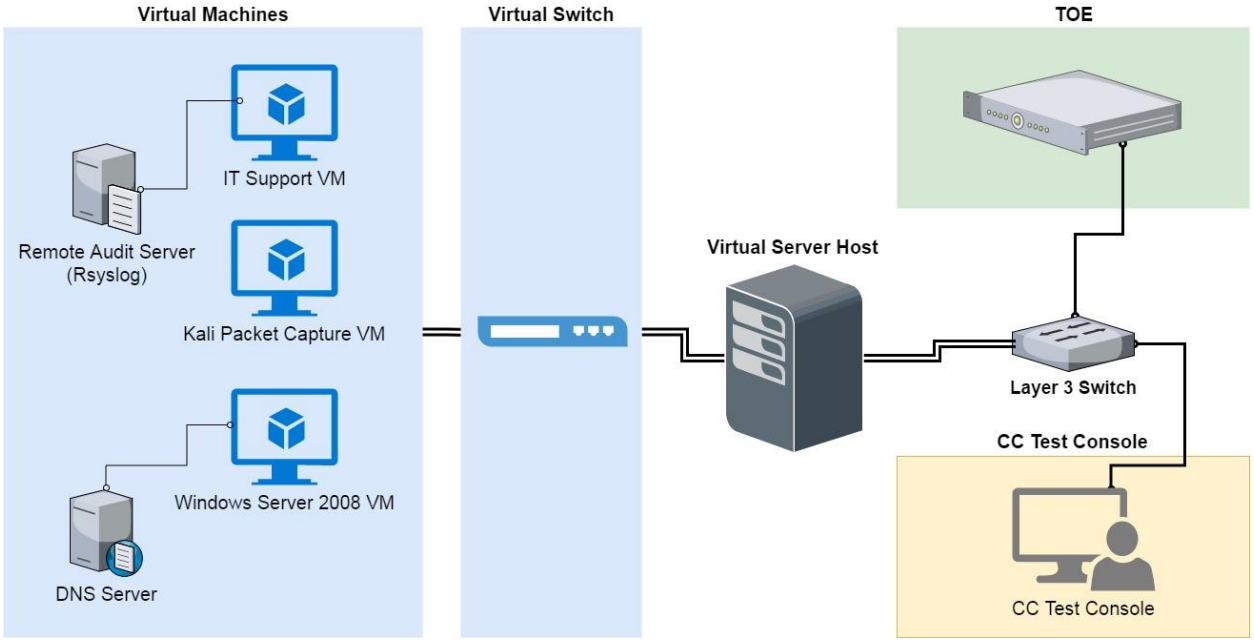

Figure 1 – Functional Testing Components Diagram

8.5 Vulnerability Analysis

The evaluation team performed a vulnerability assessment and penetration testing based on an initial port scan of the TOE. This comprehensive port scan identified all open ports and acquired all possible identifying information from the TOE. This information was compared to those services listed in the ST, and used as input into the public domain search. (This step was performed several times. For additional information, see the Evaluation Technical Report.)

Based on the output from the port scan, CVEdetails.org and ncd.nist.gov were searched with the following terms:

- Bivio
- Bivio 6310
- Bivio 6310-NC
- BiviOS
- PacStar
- PacStar 451
- RHEL 7.4
- Openssh-7.4p1-11
- Openssl-1.0.2k-8

All of the vulnerability research performed are current as of 4/17/2018.

Based on the results, no vulnerabilities exist in the TOE that are exploitable. In addition to the above information, the evaluators searched for vulnerabilities that affect installed third-party libraries. All CVEs identified either do not affect the TOE's specific version of the third-party libraries that are accessible over the network, or were mitigated by security patches installed by the vendor.

Each platform of the TOE utilizes an Intel CPU which is subject to the Specter/Meltdown hardware vulnerabilities (identified as CVE-2017-5753, CVE-2017-5715 and CVE-2017-5754). The vendor applied security patches from Red Hat Enterprise Linux, which contained both kernel, firmware and CPU-microcode security patches to address all three of the related CVEs.

9 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4

UL Verification Services Inc. has determined that the TOE meets the security criteria in the Security Target. A team of validators, on behalf of the CCEVS Validation Body, monitored the evaluation. The evaluation was completed in April 2018.

10 Validator Comments/Recommendations

The TOE does not support the use of NTP in the evaluated configuration. Administrators should ensure that NTP is not enabled in the configuration.

Note that the documentation relevant to the TOE other than the CC Guide, will be made available in a properly identified folder / directory, unique to the customer on the BIVIO support portal.

As noted in the Security Target, the product is delivered with an application that was not evaluated - this application provides non-evaluated functionality. As such, no claims can be made or inferred as to its correct operation nor should there be any assumptions made regarding any security related functionality that may be associated with this application.

Functional testing of the TOE was performed on the 6310-NC-C1M3D2N2 platform. Platform equivalency claims provided by Bivio were evaluated by the CCTL and are included in the proprietary Test Report.

11 Security Target

Bivio 6310-NC Security Target Version 1.1, April 20, 2018

12 Terms

12.1 Acronyms

CC	Common Criteria
CSP	Critical Security Parameters
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards Publication 140-2
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
I/O	Input/Output
MIB	Management Information Base
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
PP	Protection Profile
SF	Security Functions
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions

12.2 Terminology

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, Version 3.1 Revision 4, CCMB-2012-09-001.

[2] Common Criteria (CC) for Information Technology Security Evaluation – Part 2: Security functional components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-002.

[3] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, September 2012, Version 3.1, Revision 4, CCMB-2012-09-003.

[4] Common Methodology for Information Technology Security Evaluation – Evaluation methodology, September 2012, Version 3.1, Revision 4, CCMB-2012-09-004.

[5] Assurance Activity Report, VID 10873, 18-4135-R-0004, Version 1.2, April 20, 2018.

[6] Bivio 6310-NC Security Target Version 1.1, April 20, 2018

[7] Bivio 6310-NC Lifecycle and Product Labelling Q & A, Version 1.0, February 26, 2018

[8] Bivio 6310-NC Development and Design Assessment Q & A, Version 1.0, February 26, 2018

[9] Bivio 6310-NC Common Criteria Administrative Guidance, Version 1.3, March 8, 2018

[10] 18-4135-R-0002 Test Report, Version 1.2, April 20, 2018 (Evaluation Sensitive)

[11] Common Criteria Evaluation Technical Report, VID10873, 18-4135-R-0003, Version 1.1, April 20, 2018 (Evaluation Sensitive)