Indian CC Certification Scheme (IC3S)

Certification Report

Report Number	**:**	**IC3S/ MUM01/ANIPL/EAL2/0524/0042 /CR**
Product / system	:	**Array Networks AppVelocity 10_7_2_5**

Dated: 20th January 2025

Version: 1.0

Government of India
Ministry of Electronics & Information Technology
Standardization Testing and Quality Certification Directorate
6. CGO Complex, Lodi Road, New Delhi –
110003 India

This report contains a total of 16 pages. In case it needs to be reproduced, all the pages must be included.

Product developer:

Array Networks, Inc
1371 McCarthy Blvd.
Milpitas, CA 95035

TOE evaluation sponsored by:

Array Networks, Inc
1371 McCarthy Blvd.
Milpitas, CA 95035

Evaluation facility:

Common Criteria Test Laboratory (Acucert), **Mumbai**,
Acucert Labs LLP, Wing-A, Ground Floor, Beta Building, Unit No.3, iThink Techno Campus, Kanjurmarg East
Mumbai 400 042.

Evaluation Personnel:

Varsha Shetye, Acucert Labs LLP,
Sagar Pujari, Acucert Labs LLP

Evaluation report:

Evaluation Technical Report for Array Networks AppVelocity 10_7, ETR Version 0.2, 6th January 2025

Validation Personnel:

A K Upadhyaya, Scientist G, STQC, Govt. of India

Table of Contents

Contents

PART A: CERTIFICATION STATEMENT AND BACKGROUND OF THE CERTIFICATION BODY

A1 Certification Statement

The product below has been evaluated under the terms of the Indian Common Criteria Certification Scheme (IC3S) and has met the stated Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.	
Sponsor	Array Networks, Inc 1371 McCarthy Blvd. CA 95035 Milpitas, CA 95035
Developer	Array Networks, Inc 1371 McCarthy Blvd. CA 95035 Milpitas, CA 95035
The Target of Evaluation (TOE)	Array Networks AppVelocity 10_7_2_5
Security Target	Array Networks, Inc AppVelocity 10_7 Security Target Doc No: 2298-001-D102 Version: 1.2, 23 October 2024
Brief description of product	The AppVelocity 10_7 is an application delivery controller that helps optimize the interaction between clients and application servers. The application delivery controller is used within enterprise and cloud data centers and it improves the availability, security, and performance. Leveraging robust distribution algorithms, distributing the workload to multiple processors, health check mechanisms, clustering and failover capabilities, AppVelocity maintains connections, ensures persistence, directs traffic away from failed servers, and intelligently distributes application services across multiple servers for optimized performance and availability. APV can load balance traffic for a wide variety of parameters and protocols at layers 2, 3, 4 and 7, including MAC, IP address, TCP, UDP, port, http, WebSocket and WebSocket Secure. The TOE supports a vast library of policies that are hard-coded at the kernel level, are configurable with point-and-click simplicity via the Web GUI and can be combined and nested to create advanced customized application traffic management. SSL certificate/key management is also supported and can enable intelligent content management and routing. Computationally intensive key exchange and bulk encryption can also be offloaded. Management is performed via a GUI (HTTPS) or CLI (console or SSH). The TOE is virtual machine and is either delivered pre-installed on an appliance or the virtual machine can be downloaded and installed on customer hardware.
Common Criteria Standard	CC: 2022 Revision 1
CC 2022 R1 Part 2 [CC-II]	Conformant
CC 2022 R1 Part 3[CC-III]	Conformant
CC 2022 R1 Part 5 [CC-V]	Conformant
EAL	EAL2
Evaluation Lab	Common Criteria Test Laboratory, Acucert, Mumbai, India
Date Authorized	20th January 2025

A2. About the Certification Body

STQC IT Certification Services, the IT Certification Body of Standardization Testing and Quality Certification – was established in 1998 and offers a variety of services in the context of security evaluation and validation. It is the first Certification Body in India for BS 7799/ISO 27001 certification of Information Security Management Systems (ISMS). The Indian CC Certification Scheme (IC3S) is the IT security evaluation & certification Scheme based on Common Criteria standards, it is established by Govt. of India under Department of Information Technology, STQC Directorate to evaluate & certify the trustworthiness of security features in Information Technology (IT) products and systems. The IC3S is an Indian independent third party evaluation and certification scheme for evaluating the security functions or mechanisms of the IT products. It also provides framework for the International Mutual Recognition of such certificates with the member countries of CCRA (Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security). The principal participants in the scheme are:

a) Applicant (Sponsor/Developer) of IT security evaluations;
b) STQC Certification Body (STQC/MeitY/Govt. of India);
c) Common Criteria Testing Laboratories (CCTLs).

A3 Specifications of the Certification Procedure

The certification body operates under the official administrative procedures according to the criteria and procedures laid down in the following:

- ISO/IEC Guide 65, and the requirements laid down in Annex C of CCRA
- Indian Common Certification Scheme (IC3S)
- STQC/CC/DO2: Standard Operating Procedure (SOP) for Certification Body - Quality Manual – describes the quality management system for the Scheme.
- Common Criteria for Information Technology Security Evaluation (CC: 2022) part 1-5, Revision 1
- Common Evaluation Methodology (CEM: 2022), Revision 1

A4 Process of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The TOE has undergone the certification procedure at STQC IT Certification Body. The evaluation of the product was conducted by the evaluation body Common Criteria Test Laboratory (CCTL), Acucert Labs LLP, Wing-A, Ground Floor, Beta Building, Unit No.3, iThink Techno Campus, Kanjurmarg East Mumbai 400 042, India. Hereafter this has been referred as CCTL. The evaluation facility is recognized under the IC3S scheme of STQC IT Certification Body.

Array Networks, Inc 1371 McCarthy Blvd. CA 95035 Milpitas, CA 95035 is the developer and sponsor of the TOE evaluation. The certification process is concluded with the completion of this certification report.

This evaluation was completed on **06th January 2025** after submission of [**ETR**] to the certification body. The confirmation of the evaluation assurance level (EAL) only applies on the condition that

- all stated condition regarding configuration and operation, as given in part B of this report, are observed,
- The product is operated – where indicated – in the operating environment described.

This certification report applies only to the version and release of the product indicated here. The validity of the certificate can be extended to cover new versions and releases of the product, provided the applicant applies for re-certification of the modified product, in accordance with the procedural requirements, and provided the evaluation does not reveal any security deficiencies.

A5 Publication

The following Certification Results consist of Sections B1 to B11 of this report. The TOE will be included in the list of the products certified under IC3S Scheme of STQC IT Certification Body. The list of certified products is published at regular intervals in the Internet at http://www.commoncriteria-india.gov.in. Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form on request to the Certification Body.

PART B: CERTIFICATION RESULTS

B.1 Executive Summary

B.1.1 Introduction

The Certification Report documents the outcome of Common Criteria security evaluation of the TOE. It presents the evaluation results and the conformance results. This certificate is intended to assist the prospective buyers and users when judging the suitability of the IT security of the product for specified requirements.

Prospective buyers and users are advised to read this report in conjunction with the referred [ST] of the product, which specifies the functional, environmental and assurance requirements.

The evaluation was performed by Common Criteria Test Laboratory (CCTL), Acucert Labs LLP, Wing-A, Ground Floor, Beta Building, Unit No.3, iThink Techno Campus, Kanjurmarg East Mumbai 400 042, India. The information in the test report is derived from the [ST] written by the developer and the Evaluation Technical Report [ETR] written by Common Criteria Test Laboratory [Acucert Labs LLP, Wing-A, Ground Floor, Beta Building, Unit No.3, iThink Techno Campus, Kanjurmarg East Mumbai 400 042, India]. The evaluation team determined the product to be CC: 2022 R1, Part 2 and Part 3 conformant and concluded that the Common Criteria requirements for Evaluation Assurance Level (**EAL 2**) have been met.

B 1.2 Evaluated product and TOE

The TOE consists of Array Networks AppVelocity 10_7_2_5 software which is either

1. Virtual appliance running on the AVX series x900.
2. Virtual appliance running on the APV series x900.

The following software, hardware and networking components are not included in the evaluation of the TOE but required for operation of the TOE in the evaluated configuration.

Table 1 – Non-TOE Hardware and Software

Component	**Software**	**Hardware**
Host Server (hosting TOE)	KVM (Kernel-based Virtual Machine) server software in CentOS 6.0 or later	APV x900 or AVX x900 hardware
Administrator Workstation	Operating system supporting Chrome 122.0 or later, or Firefox 123.0 or later	General Purpose Computer Hardware
Syslog server	Software supporting RFC5424	General Purpose Computer Hardware

MD5 Hash value: ad58d66eca5f2d33bf686d1a3731d223
SHA256 Hash value: 5a8a57401797c24c9854bbe91e98465cbf5720ce5a67a350bc61e111b5d3b9f4

The evaluated sub-set and configuration of the product is described in this report as the Target of Evaluation (TOE). The Evaluated Configuration, its security functions, assumed environment, architectural information and evaluated configuration are given below (Refer B2 to B5).

B 1.3 Security Claims

The [ST] specifies the security objectives of the TOE and the threats that they counter (Refer 4.1 and 3.1 of ST). All the

Security Functional Requirements (SFRs) (listed in 6.2 of ST) are taken from CC Part 2 are included.

B 1.4 Conduct of Evaluation

The evaluation was initiated by the IC3S Certification Scheme of STQC IT Certification Body vide communication no. IC3S/CB/0524/0042 dated 14th May 2024.

The TOE as described in the [ST] is Array Networks AppVelocity 10_7_2_5 software which is a virtual machine and is either delivered pre-installed on an appliance (AVX series x900 or APV series x900) or the virtual machine can be downloaded and installed on AVX series x900 or APV series x900 customer hardware. The TOE was evaluated through evaluation of its documentation; testing and vulnerability assessment using methodology stated in Common Evaluation Methodology [CEM] and Acucert Common Criteria Test Procedures (ACU/AMS/TP/001 version 2.1).

The evaluation has been carried out under written agreement [22nd May 2024] between Common Criteria Test Laboratory, Acucert, Mumbai and the sponsor.

B 1.5 Independence of Certifier

The certifier did not render any consulting or other services for the company ordering the certification and there was no relationship between them, which might have an influence on this assessment.

B 1.6 Disclaimers

The certification results only apply to the version and release of the product as indicated in the certificate. The certificate is valid for stated conditions as detailed in this report. This certificate is not an endorsement of the IT product by the Certification Body or any other organization that recognizes or gives effect to this certificate. It is also not an endorsement of the target of evaluation (TOE) by any agency of the Government of India and no warranty of the TOE is either expressed or implied.

B 1.7 Recommendations and conclusions

- The conclusions of the Certification Body are summarized in the Certification Statement at Section A1.
- The specific scope of certification should be clearly understood by reading this report along with the [ST].
- The TOE should be used in accordance with the environmental assumptions mentioned in the [ST].
- The TOE should be used in accordance with the supporting guidance documentation.
- This Certification report is only valid for the evaluated configurations of the TOE.

B2 Identification of TOE

The Array Networks AppVelocity 10_7_2_5 (APV) is an application delivery controller that helps optimize the interaction between clients and application servers. The application delivery controller is used within enterprise and cloud data centers and it improves the availability, security, and performance.

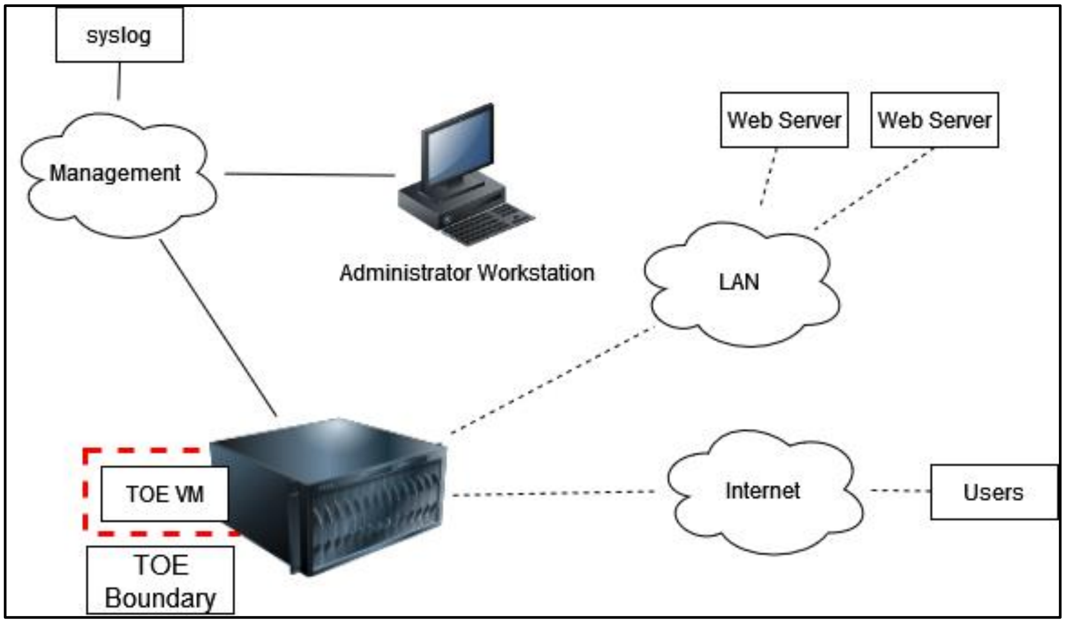
APV can load balance traffic for a wide variety of parameters and protocols at layers 2, 3, 4 and 7, including MAC, IP address, TCP, UDP, port, http, WebSocket and WebSocket Secure.

The TOE supports a vast library of policies that are hard-coded at the kernel level, are configurable with point-and-click simplicity via the Web GUI and can be combined and nested to create advanced customized application traffic management. SSL certificate/key management is also supported and can enable intelligent content management and routing. Computationally intensive key exchange and bulk encryption can also be offloaded.

Management is performed via a GUI (HTTPS) or CLI (console or SSH).

The TOE is virtual machine and is either delivered pre-installed on an appliance (AVX series x900 or APV series x900) or the virtual machine can be downloaded and installed on customer hardware.

A typical TOE deployment is shown in the figure below.



TOE Deployment

The following software, hardware and networking components are not included in the evaluation of the TOE but required for operation of the TOE in the evaluated configuration.

Component	**Software**	**Hardware**
Host Server (hosting TOE)	KVM (Kernel-based Virtual Machine) server software in CentOS 6.0 or later	APV x900 or AVX x900 hardware
Administrator Workstation	Operating system supporting Chrome 122.0 or later, or Firefox 123.0 or later	General Purpose Computer Hardware
Syslog server	Software supporting RFC5424	General Purpose Computer Hardware

B2.1 Deliverables to be provided by the Developer to the End-user:

The TOE is a virtual machine and once purchased it can be downloaded from the Array Networks support site. Customers are provided with an account and can download the virtual machine (in a zip file) and the guidance documentation (pdf format). The x900 appliances with the pre-installed TOE are delivered via commercial courier.

The guidance documentation can be found by searching for the document on the Array Networks support site which has the current version of each document. The TOE includes the following documentation in pdf format:

- AVX5900 Quick Installation Guide, March 14, 2024
- AVX7900/9900 Quick Installation Guide, March 14, 2024
- APV5900 Quick Installation Guide, March 14, 2024
- APV7900/9900 Quick Installation Guide, March 14, 2024
- ArrayOS APV 10.7 User Guide, April 22, 2024
- ArrayOS AVX 2.7 User Guide
- ArrayOS APV 10.7 CLI Handbook, May 14, 2024
- AppVelocity vAPV Administration Guide, September 10, 2020
- Array Networks AppVelocity 10_7 Common Criteria Guidance Supplement, v0.7, 23 October 2024

B3 Security policy

There are following organizational security policies that the TOE must meet (Given in table 2 below).

Table 1: Organizational Security Policies

OSP	Description
P.MANAGE	The TOE shall be managed only by authorized users.
P.ACCOUNT	The authorized users of the TOE shall be held accountable for their actions within the TOE.

B.4 Assumptions

There are following assumptions exist in the TOE environment.

Table 2: Assumptions

Assumption	Description
A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.

B.5 Evaluated configuration

The TOE is a virtual machine and once purchased it can be downloaded from the Array Networks support site. Customers are provided with an account and can download the virtual machine (in a zip file). The physical scope of the TOE consists of the TOE software. The TOE is virtual machine and is either delivered pre-installed on an appliance (AVX series x900 or APV series x900) or the virtual machine can be downloaded and installed on customer hardware. The evaluated configuration is given in table 4 below:

Table 4: Details of evaluated configuration of the TOE

Description	Software Version and Release	Hash values of the image files
Array Networks AppVelocity 10_7_2_5	Version 10_7_2_5	MD5 Hash value: ad58d66eca5f2d33bf686d1a3731d223 SHA256 Hash value: 5a8a57401797c24c9854bbe91e98465cbf5720ce5a67a350bc61e111b5d3b9f4

B6 Document Evaluation

B.6.1 Documentation

The list of documents, those were presented, as evaluation evidences to the evaluators at the evaluation facility, are given below:

1. **Security Target**: Array Networks, Inc AppVelocity 10_7 Security Target Doc No: 2298-001-D102 Version: 1.2, 23 October 2024
    1. **TOE Architecture:** Array Networks AppVelocity 10_7 Development Version: 1.0 23 October 2024 Doc No.: 2298-001-D104
    2. **TOE Functional Specification:** Array Networks AppVelocity 10_7 Development Version: 1.0 23 October 2024 Doc No.: 2298-001-D104
    3. **TOE Design description**: Array Networks AppVelocity 10_7 Development Version: 1.0 23 October 2024 Doc No.: 2298-001-D104
    4. **Preparative Guidance**:
        - APV5900 Quick Installation Guide Last Update: March 14, 2024
        - APV7900/9900 Quick Installation Guide Last Update: March 14, 2024
        - AVX5900 Quick Installation Guide Last Update: July 11, 2024
        - AVX7900 Quick Installation Guide Last Update: July 11, 2024
        - AVX9900 Quick Installation Guide Last Update: July 11, 2024
    5. **Operational Guidance**:
        - Array Networks AppVelocity 10_7 Common Criteria Guidance Supplement Version: 0.7 3 October 2024 Doc No.: 2298-001-D105
        - vAPV Administration Guide For ArrayOS APV 10.4 Release September 10, 2020
        - ArrayOS APV 10.7 CLI Handbook Last Update: May 14, 2024
        - ArrayOS APV 10.7 User Guide Last Update: April 22, 2024
        - ArrayOS AVX 2.7.2 User Guide Last Update: March 21, 2024
    6. **Configuration Management Capability:** Array Networks AppVelocity 10_7 Life-Cycle Support Version: 0.8 23 October 2024 Doc No.: 2298-001-D106
    7. **Configuration Management Scope:** Array Networks AppVelocity 10_7 Life-Cycle Support Version: 0.8 23 October 2024 Doc No.: 2298-001-D106
    8. **TOE delivery:** Array Networks AppVelocity 10_7 Life-Cycle Support Version: 0.8 23 October 2024 Doc No.: 2298-001-D106
    9. **Test cases, logs and coverage**:
        - Array AppVelocity 10_7 Developer Test Report for APV 1900 Version 0.3 11/12/2024
        - Array AppVelocity 10_7 Developer Test Report for AVX vAPV Version 0.3 11/12/2024

B.6.2 Analysis of document

The documents related to the following areas were analyzed using [CEM]. The summary of analysis is as below:

Development process: The evaluators analyzed the functional specification of the TOE and found that the TOE security function interfaces are described clearly and unambiguously. The evaluators also analyzed design and architectural descriptions of the TOE and determined that the TOE (Array Networks AppVelocity

10_7_2_5) software) is clearly described in the design description. The evaluators determined that architectural description of the TOE includes secure initialization and also means of protection of the TOE from tampering and bypassing.

Guidance Documents: The evaluators analysed guidance documents like preparative procedure and operational user guidance and determined that preparative procedure describes clear and unambiguous steps to bring the TOE to its secure state. The operational user guidance information were also clear and unambiguous.

Life-cycle support documents: The Life cycle support process document, containing information on Configuration Management and Delivery Procedure were evaluated.

Configuration management: The evaluators analyzed configuration management documentation and determined that the TOE and its associated documents are clearly identified as configurable items. The evaluators also analyzed access control measures defined in the documentation and found satisfactory**.**

Delivery procedure: The delivery procedure document was audited with the objective to ascertain whether it covers secure delivery of the TOE to the end-users. The secure delivery procedure has been described in the document and the same has been audited by the evaluators during their virtual site visit. The end-users can check integrity of the evaluated TOE using hash value of that, if felt necessary.

The final version of the respective evaluation evidences was found to comply with the requirements of CC 2022 R1 for EAL2.

B7 Product Testing

Testing at EAL2 consists of the following three steps: Testing by developer, Independent Testing by Evaluation Team, and Penetration testing.

B 7.1 IT Product Testing by Developer

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the [ETR].

The evaluators analysed the developer's test coverage and found them to be complete and satisfactory. The correspondence between the tests identified in the developer's test documentation and the functional specification and TOE design was complete.

B 7.2 IT Product Independent Testing by Evaluation Team

The evaluators' independent functional testing effort is summarized as below.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and reproducibility of results.

The TOE has been installed properly as per the preparative procedure document.

The evaluators have repeated the developer's test at CCTL (Acucert), Mumbai to confirm the reproducibility of the test results.

While making the test strategy for independent testing, consideration is given to cover the security requirements, as well as the security specification as defined in the security target, interfaces available to the users to cover each of security functional requirements, TOE design and security architecture information. Independent testing is designed to verify the correct implementation of security functionalities available to different levels of users and to check whether audit is being generated for auditable events.

The evaluators test effort is summarized as below:

#	Aspects	Evaluator's comments
1	On overall evaluator testing strategy & approach	The evaluators simulated all of the developers' tests and found that those are reproducible; in addition to that they developed test cases that augment the developer tests and conducted most of those cases independently at CCTL (Acucert), Mumbai.
2	On TOE test configurations: The particular configurations of the TOE that were tested, including whether any privileged code were required to set up the test or clean up afterwards.	The evaluators have examined the TOE and it was found to be configurable as per the description given in the developer's preparative guidance document. It is also observed that the test configuration is consistent with the description as given in the security target document. The TOE was installed properly as per the preparative procedure AGD_PRE document.
3	On depth of testing in respect of all functionalities of all TSFs	The evaluators have repeated all the test objectives of developer's tests at CCTL (Acucert), Mumbai to verify the reproducibility of test results and to ensure the coverage of all TSFIs, as mentioned in the FSP document. In addition to that they developed test cases that augment the developer tests and conducted most of those cases independently at CCTL (Acucert), Mumbai. Highlights of Independent testing are given below: • The TOE was installed properly as per the preparative procedure AGD_PRE document. • The evaluators have repeated the developer's test at CCTL (Acucert), Mumbai to confirm the reproducibility of the test results. While making the test strategy for independent testing, consideration is given to cover the security requirements as defined in the security target, visible interfaces available to the users to cover each of security functional requirements, TOE design information and its security architecture. Independent testing is designed to verify the correct implementation of security functionalities available to different levels of users and to check whether audit is being generated for auditable events.
4	On test results: A description of the overall evaluator testing results	The evaluator conducted tests on the TOE executable delivered by the developer and found to be in compliance with the ST.

B 7.3 Vulnerability Analysis and Penetration testing

Evaluators searched over internet for potential vulnerabilities of AppVelocity 10_7 (Rel_APV_10_7_2_5) software. The following urls were explored:

- https://nvd.nist.gov/view/vuln.search
- http://cve.mitre.org/cve
- https://www.cvedetails.com/vulnerability-search.php
- https://www.kb.cert.org/vuls/search/
- www.exploitsearch.net
- www.securiteam.com
- http://nessus.org/plugins/index.php?view=search
- http://www.zerodayinitiative.com/advisories
- https://www.exploit-db.com
- https://www.rapid7.com/db/vulnerabilities

There was no exploitable vulnerability found in this version of the product with Basic attack potential.

Further, by using Nessus Vulnerability scanner, no exploitable vulnerabilities were found. With Nmap and Fuzz testing also no vulnerabilities could be found.

The TOE documents like, Security Target (ST), TOE architecture & Design (TDS), TOE Preparatory guidance document etc. were analyzed to find out potential security vulnerabilities and the same are listed out below:

AT1: ***An expert who is conversant in IT technology would be able to succeed in an attack within two weeks by modifying and applying an attack tool available on the internet***

AT2: ***An attacker could flood the target system (TSF) with excessive traffic, overwhelming its resources and preventing legitimate users from accessing it***

AT3: Audit record mechanism can be tampered by consuming audit storage space.

AT4: An attacker could intercept communications between the target system and other systems to eavesdrop on or manipulate data (MiTM Attack).

AT5: An attacker could gain unauthorized access to the system by using brute force attacks or password guessing techniques to compromise user accounts and gain access to network resources.

The attack potential for each of the vulnerabilities was calculated using guidance given in CEM:2022 R1 and considering various factors like the time to identify & exploit the vulnerability, expertise required, knowledge of the TOE, windows of opportunity and equipment requirement.

The attack potential for each of the 5 attack scenarios were calculated and all of them have the score >10. Thus, none of attack scenarios can be exploited with Basic attack potential.

The evaluator conducted no Penetration Testing as all the identified attack scenarios had Attack potential > 10 (Beyond Basic).

Hence, it is concluded that the TOE does not contain any exploitable vulnerability for 'Basic Attack Potential'.

B 8 Evaluation Results

The evaluation results have been documented in the [ETR].

Report No: Evaluation Technical Report for Array Networks AppVelocity 10_7 ETR Version 0.2, 6th January 2025

The TOE was evaluated through evaluation of its documentation, testing and vulnerability assessment using methodology stated in [CEM] and Acucert Common Criteria Test Procedures (ACU/AMS/TP/001 version 2.1).

Documentation evaluation results:

The documents for TOE and its development life cycle were analyzed by the evaluator in view of the requirements of the respective work units of the [CEM]. The final versions of the documents were found to comply with the requirements of CC 2022 R1 for EAL 2.

Testing:

The developer’s tests and the independent functional tests yielded the expected results, giving assurance that ‘**AppVelocity 10_7 (Rel_APV_10_7_2_5)**’, behaves as specified in its [ST], functional specification and TOE design.

Vulnerability assessment and penetration testing:

There were no vulnerabilities with ‘**Basic**’ attack potential as identified through vulnerability assessment. Hence no penetration testing was carried out.

B 9 Validator Comments

The Validators have reviewed the Evaluation Technical Report [ETR] along with all relevant evaluation evidences, documents, records, etc. and are in agreement with the conclusion made in it i.e.

- **The [ST] Array Networks, Inc AppVelocity 10_7 Security Target Doc No: 2298-001-D102 Version: 1.2, 23 October 2024 has satisfied all the requirements of the assurance class ASE.**
- **The results of evaluation of product and process documentation, testing and vulnerability assessment confirm that AppVelocity 10_7 (Rel_APV_10_7_2_5), satisfies all the security functional requirements and assurance requirements as defined in the [ST]. Hence, the TOE is recommended for EAL2 Certification**.

However, it should be noted that there are no **Protection Profile** compliance claims.

B 10 List of Acronyms

ACL: Access Control List
CC: Common Criteria
CCTL: Common Criteria Test Laboratory
CEM: Common Evaluation Methodology
DVS: Development security
EAL: Evaluation Assurance Level ETR: Evaluation
Technical Report FSP: Functional Specification
IC3S: Indian Common Criteria Certification Scheme
IT: Information Technology

PP: Protection Profile ST: Security Target

TOE: Target of Evaluation

TDS: TOE Design Specification

TSF: TOE Security Function

TSFI: TOE Security Function Interface

B 11 References

1. [CC-I]: CC: 2022 R1: Part 1: Introduction and general model
2. [CC-II]: CC: 2022 R1: Part 2: Security functional components
3. [CC-III]: CC: 2022 R1: Part 3: Security assurance components
4. [CC-IV]: CC: 2022 R1: Part 4: Framework for the specification of evaluation methods and activities
5. [CC-V]: CC: 2022 R1: Part 5: Pre-defined packages of security requirements
6. [CEM]: CEM: 2022 R1: Evaluation Methodology
7. [ST]: Array Networks, Inc AppVelocity 10_7 Security Target Doc No: 2298-001-D102 Version: 1.2, 23 October 2024
8. [ETR]: Evaluation Technical Report for Array Networks AppVelocity 10_7 ETR Version 0.2, 6th January 2025
9. [ACU/AMS/TP/001]: Acucert Common Criteria Test Procedures (version 2.1).