National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

CACI Archon OS v3.0.0.2

Report Number:	**CCEVS-VR-VID11429-2024**
Dated:	**July 12, 2024**
Version:	**0.2**

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

Chris Thorpe
Clare Parran
Linda Morrison
Lisa Mitchell
Lori Sarem
Randy Heimann

The MITRE Corporation

Common Criteria Testing Laboratory

Fathi Nasraoui
Chaitanya Muzumdar
Snehal Gaonkar
Theo Ajibade

Intertek 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 CACI Archon OS v3.0.0.2 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 July 2024. 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 Extended and meets the assurance requirements of the *Protection Profile for General Purpose Operating Systems*, Version 4.3, 27 September 2022 and *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019.

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 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 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	Archon OS v3.0.0.2
Protection Profile	*Protection Profile for General Purpose Operating Systems*, Version 4.3, 27 September 2022. *Functional Package for Transport Layer Security (TLS),* Version 1.1, 01 March 2019.
Security Target	*CACI Archon OS v3.0.0.2 Security Target v1.5*
Evaluation Technical Report	*Evaluation Technical Report for CACI Archon OS v3.0.0.2*
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Extended
Sponsor	CACI
Developer	CACI
Common Criteria Testing Lab (CCTL)	Intertek Acumen Security Rockville, MD
CCEVS Validators	Randy Heimann: Lead Validator Clare Parran: Lead Validator Chris Thorpe: Senior Validator Linda Morrison: Validator Lisa Mitchell: Validator Lori Sarem: Validator

3 Architectural Information

3.1 TOE overview

Archon OS is an operating system (OS) based on Red Hat Enterprise Linux (RHEL) v8.10 that supports multiple users, user permissions, access controls, and cryptographic functionality.

Archon OS is an ostree-based packaging of Red Hat Enterprise Linux (RHEL), tailored for deployment on End User Devices (EUDs) specifically designed for Commercial Solutions for Classified (CSfC) solutions. The Archon OS ostree incorporates unmodified versions of the RHEL RPMs. Archon OS is curated to incorporate solely the essential OS options and applications pertinent to EUD functionality, with non-applicable components deliberately excluded.

3.2 Evaluated Configuration

The TOE is a software TOE and has been evaluated on the following host platforms.

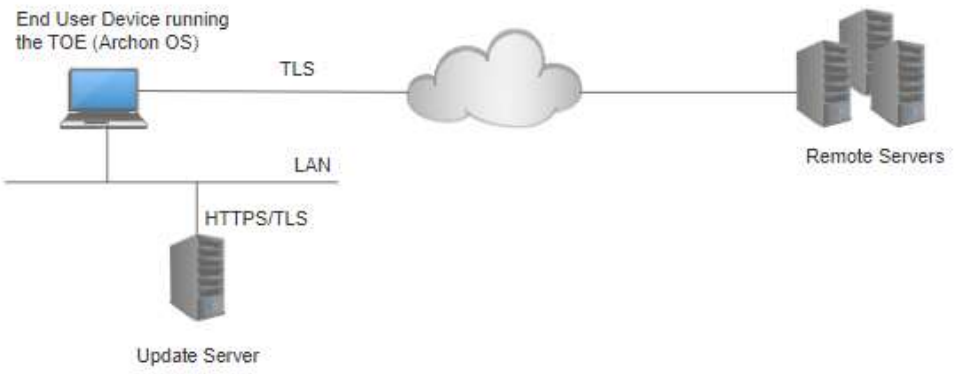
Table 2 – Archon OS v3.0.0.2 Hardware Platforms (EUDs)

Vendor	Model	CPU	CPU Microarchitecture	CPU Family
Dell Inc.	Latitude 5400	Intel® Core™ i5-8365U	Skylake	Whiskey Lake
	Latitude 5410	Intel® Core™ i7-10810U	Skylake	Comet Lake
	Latitude 5430	Intel® Core™ i7-1255U	Golden Cove	Alder Lake
	Precision 3260	Intel® Core™ i7-12700	Golden Cove	Alder Lake
	Precision 3570	Intel® Core™ i7-1255U	Golden Cove	Alder Lake
	Latitude 5440	Intel® Core™ i5-1335U	Raptor Cove	Raptor Lake
	Latitude 5540	Intel® Core™ i5-1335U	Raptor Cove	Raptor Lake
	Precision 3580	Intel® Core™ i5-1350P	Raptor Cove	Raptor Lake

3.3 Physical Boundaries

The diagram below depicts a representative TOE deployment.

Figure 1: Representative TOE Deployment



The following items are required for the operational environment.

Table 3: Hardware and Software Environmental Components

Components	Mandatory/ Optional	Description
End User Device (EUD)	Mandatory	The hardware runs the TOE (software). The evaluated systems are identified in Table 2 above.
Update Server	Mandatory	Provides the ability to check for TOE software updates TOE as well as providing signed updates. The TOE communicates with the Update Server using HTTPS over TLS.
Remote Servers	Mandatory	Servers that support multiple applications and provide multiple services.

3.4 TOE's Excluded Functionality

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

- SELinux Mandatory Access Control System
- OS Virtualization Infrastructure
- Containerization infrastructure

4 Security Policy

The TOE provides the security functions required by *Protection Profile for General Purpose Operating Systems*, Version 4.3 (PP_OS_V4.3) and *Functional Package for Transport Layer Security (TLS),* Version 1.1 (PKG_TLS_V1.1).

4.1 Security Audit

The TOE generates and stores audit events using the Lightweight Audit Framework (LAF). The LAF is designed to be an audit system making Linux compliant with the requirements from Common Criteria by intercepting all system calls and retrieving audit log entries from privileged user space applications. The framework allows configuring the events to be recorded from the set of all events that are possible to be audited. Each audit record contains the date and time of event, type of event, subject identity, user identity, and result (success/fail) of the action if applicable.

4.2 Cryptographic Support

The TOE provides a broad range of cryptographic support, providing TLSv1.2 protocol implementation in addition to individual cryptographic algorithms. The cryptographic services provided by the TOE are described below and in full detail in Section 6.2 of this document.

The TOE includes the OpenSSL v1.1.1k and the Linux Cryptographic API libraries, and each cryptographic algorithm has been validated for conformance to the requirements specified in their respective standards and awarded a CAVP certificate as identified in ST.

The OpenSSL library provides the TLS Client function. The OpenSSL library also provides cryptographic algorithms for the trusted update and secure boot security functions.

The TOE provides two SP800-90A-compliant DRBG for creation of key components of asymmetric keys and random number generation. One CTR_DRBG is provided by the OpenSSL cryptographic module in application space and one HMAC_DRBG is provided by a Cryptographic Kernel API module located in the Kernel space.

4.3 User Data Protection

Discretionary Access Control (DAC) allows the TOE to assign owners to file system objects and Inter-Process Communication (IPC) objects. The owners are allowed to modify Unix-type permission bits for these objects to permit or deny access for other users or groups. The DAC mechanism also ensures that untrusted users cannot tamper with the TOE mechanisms.

The TOE also implements Portable Operating System Interface (POSIX) Access Control Lists (ACLs) that allow the specification of the access to individual file system objects down to the granularity of a single user.

4.4 Identification and Authentication

User identification and authentication in the TOE includes all forms of interactive login (e.g., log in at the local console) as well as identity changes through the su or sudo commands. These all rely on explicit authentication information provided interactively by a user.

The authentication security function allows password-based authentication.

Password quality enforcement mechanisms are offered by the TOE which are enforced at the time when the password is changed.

4.5 Security Management

The security management facilities provided by the TOE are usable by authorized users and/or authorized administrators to modify the configuration of TSF.

4.6 TOE Access

The TOE displays informative banners before users are allowed to establish a session.

4.7 Protection of the TSF

The TOE implements self-protection mechanisms that protect the security mechanisms of the TOE as well as software executed by the TOE. The following kernel-space isolation and TSF self-protection mechanisms are implemented and enforced (full details are provided in the TSS):

- Address Space Layout Randomization for user space code.
- Kernel and user-space ring-based separation of processes.
- Stack buffer overflow protection using stack canaries.
- Secure Boot ensures that the boot chain up to and including the kernel together with the boot image (initramfs) is not tampered with.
- Updates to the operating system are only installed after their signatures have been successfully validated.
- Application Whitelisting restricts execution to known/trusted applications.

4.8 Trusted Path/Channels

The TOE supports TLSv1.2 to secure remote communications.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

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

Table 4: Assumptions

ID	Description
A.PLATFORM	The OS relies upon a trustworthy computing platform for its execution. This underlying platform is out of scope of this PP.
A.PROPER_USER	The user of the OS is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy. At the same time, malicious software could act *as* the user, so requirements which confine malicious subjects are still in scope.
A.PROPER_ADMIN	The administrator of the OS is not careless, willfully negligent or hostile, and administers the OS within compliance of the applied enterprise security policy.

5.2 Threats

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

Table 5: Threats

ID	Description
T.NETWORK_ATTACK	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with applications and services running on or part of the OS with the intent of compromise. Engagement may consist of altering existing legitimate communications.
T.NETWORK_EAVESDROP	An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between applications and services that are running on or part of the OS.
T.LOCAL_ATTACK	An attacker may compromise applications running on the OS. The compromised application may provide maliciously formatted input to the OS through a variety of channels including unprivileged system calls and messaging via the file system.
T.LIMITED_PHYSICAL_ACCESS	An attacker may attempt to access data on the OS while having a limited amount of time with the physical device.

5.3 Clarification of Scope

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

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the *Protection Profile for General Purpose Operating Systems*, Version 4.3, 27 September 2022 *and Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019.
- 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.
- 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:

- [ST] CACI *Archon OS v3.0.0.2 Security Target*, Version 1.5, July 4, 2024
- [CCSupl] CACI *Archon OS v3.0.0.2 Common Criteria User Guidance v1.2*

7 Conformance Claims

7.1 CC Conformance Claims

The TOE is conformant to the following:

- *Common Criteria for Information Technology Security Evaluations Part 2*, Version 3.1, Revision 5, April 2017 extended.
- *Common Criteria for Information Technology Security Evaluations Part 3*, Version 3.1, Revision 5, April 2017 extended.

7.2 Protection Profile Conformance

This ST claims exact conformance to the following CC specifications:

- *Protection Profile for General Purpose Operating Systems*, Version 4.3, 27 September 2022 with the Strictly Optional SFR, FTA_TAB.1 and the Objective SFR, FPT_SRP_EXT.1 included.
- *Functional Package for Transport Layer Security (TLS),* Version 1.1, 01 March 2019 with the following selection based SFRs included.
  - FCS_TLSC_EXT.1
  - FCS_TLSC_EXT.2
  - FCS_TLSC_EXT.4
  - FCS_TLSC_EXT.5

7.3 Conformance Rationale

The security requirements in this Security Target are all taken from the Protection Profile and Functional Package performing only operations defined there. All mandatory SFRs are claimed. The PP_OS_V4.3 and PKG_TLS_V1.1 Selection-Based SFRs are claimed and are consistent with the selections made in the mandatory SFRs that prompt their inclusion. The additional SFRs claimed in the ST are identified in section 7.2 above.

7.3.1 Technical Decisions

The following table identifies the NIAP Technical Decisions that apply to the TOE and have been accounted for in the ST development and the conduct of the evaluation or were considered to be non-applicable.

Table 6: Relevant Technical Decisions

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable) and Notes
GPOS PP v4.3		
TD0839: Clarification for Local Administration in FTP_TRP.1.3	Yes	Modifies FTP_TRP.1.3 SFR, Application Note, TSS, AGD, and Test.
TD0821: Corrections to ECD for PP_OS_V4.3	Yes	
TD0812: Updated CC Conformance Claims in PP_OS_V4.3	Yes	
TD0809: Update to FCS_COP.1/SIGN for CNSA 1.0 compliance with secure Boot Exception	Yes	Modifies FCS_COP.1/SIGN SFR, TSS, and AGD. Archives TD0727

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable) and Notes
TD0789: Correction to TLS Selection in FIA_X509_EXT.2.1	Yes	Modifies FIA_X509_EXT.2.1 SFR and Test. Modifies FTP_ITC_EXT.1.1 SFR, Application Note, and Test.
TD0773: Updates to FIA_X509_EXT.1 for Exception Processing and Test Conditions	Yes	Modifies FIA_X509_EXT.1.1 Application Note, TSS, and Test. Archives TD0692
TD0713: Functional Package SFR mappings to objectives	Yes	
TD0712: Support for Bluetooth Standard 5.3	Yes	Modifies FCS_CKM.1 SFR, Application Note, TSS, AGD, and Test. Modifies FCS_COP.1/ENCRYPT SFR, Application Note, TSS, and Test.
TD0701: Incomplete selection reference in FCS_CM_EXT.4 TSS activities	Yes	Applies to FCS_CKM_EXT.4 TSS AA.
TD0696: Removal of 160-bit selection from FCS_COP.1/HASH & FCS_COP.1/KEYMAC	Yes	Modifies FCS_COP.1/HASH and FCS_COP.1.1/KEYHMAC SFRs.
TD0693: Typos in OSPP 4.3	Yes	Applies to FMT_MOF_EXT.1 Application Note, FMT_SMF_EXT.1 Application Note, and FMT_SMF_EXT.1 Application Note. Applies to FAU_GEN.1 Test.
TD0691: OSPP 4.3 Conditional authentication testing	Yes	Applies to FIA_AFL.1 Application Note and Test.
TD0675: Make FPT_W^X_EXT.1 Optional	Yes	
TLS Pkg v1.1		
TD0779: Updated Session Resumption Support in TLS package V1.1	Yes	The ST does not claim TLS server, however the TD Archives TD0588 and therefore applies to this evaluation.
TD0770: TLSS.2 connection with no client cert	No	The ST does not claim TLS server.
TD0739: PKG_TLS_V1.1 has 2 different publication dates	Yes	The TD modifies FCS_TLSS_EXT.1.3 Test which doesn't apply to this evaluation, but also mentions the two different dates for PKG_TLS_V1.1 (https and pdf) and that 03.01.2019 should be used and therefore the TD applies to this evaluation.
TD0726: Correction to (D) TLSS SFRs in TLS 1.1 FP	No	The ST does not claim TLS or DTLS server.
TD0513: CA Certificate loading	Yes	Applies to FCS_TLSC_EXT.1.3 Test.
TD0499: Testing with pinned certificates	Yes	Applies to FCS_TLSC_EXT.1.2 Test.

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable) and Notes
TD0469: Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1	No	The ST does not claim TLS server.
TD0442: Updated TLS Ciphersuites for TLS Package	Yes	Modifies FCS_TLSC_EXT.1.1 SFR.

8 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 Archon OS, which is not publicly available. The AAR 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 to the vendor-provided guidance documentation and ran the tests specified in the Protection Profile for General Purpose Operating Systems, Version 4.3, 27 September 2022 and Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019. The Independent Testing activity is documented in the AAR, which is publicly available, and is not duplicated here.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the 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 determined the TOE Name to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP.

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 Archon OS 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 Protection Profile for General Purpose Operating Systems, Version 4.3, 27 September 2022 and Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019.

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

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 ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the Protection Profile for General Purpose Operating Systems, Version 4.3, 27 September 2022 and Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 related to the examination of the information contained in the TOE Summary Specification.

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

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 Protection Profile for General Purpose Operating Systems, Version 4.3, 27 September 2022 and Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019 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

The evaluation team applied each EAL 1 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

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 *Protection Profile for General Purpose Operating Systems*, Version 4.3, 27 September 2022 and *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019 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 Protection Profile for General Purpose Operating Systems, Version 4.3, 27 September 2022 and Functional Package for Transport Layer Security (TLS), Version 1.1, 01 March 2019, 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 evaluator examined sources of publicly available information to identify potential vulnerabilities in the TOE. The sources examined are as follows:
    - **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**

The evaluator examined public domain vulnerability searches by performing a keyword search. The terms used for this search were based on the vendor's name, product name, and key platform features leveraged by the product. As a result, the evaluator performed a search using the following keywords:

- CACI
- archon-os
- archon
- Red Hat Enterprise Linux 8.10
- aide-0.16-14.el8_5.1s
- TLSV1.2
- audit-libs-3.1.2-1.el8
- chrony-4.5-1.el8
- cryptsetup-libs-2.3.7-7.el8
- curl-7.61.1-34.el8
- dnf-4.7.0-20.el8
- fapolicyd-1.3.2-1.el8
- firewalld-0.9.11-4.el8
- gpgme-1.13.1-12.el8
- grub2-common-2.02-156.el8
- gnutls-3.6.16-8.el8_9.3
- gzip-1.9-13.el8_5
- iptables-1.8.5-11.el8_9
- kernel-4.18.0-533.el8_10
- libcap-2.48-6.el8_9.
- libcap-ng-0.7.11-1.el8
- libpcap-1.9.1-5.el8
- openldap-2.4.46-18.el8
- openssh-8.0p1-24.el8.
- openssl-1.1.1k-12.el8_9.
- ostree-libs-2022.2-8.el8.
- pam-1.3.1-33.el8.x86_64
- polkit-0.115-15.el8_10.2.
- rpm-4.14.3-31.el8.x86_64
- rsyslog-8.2102.0-15.el8.
- sudo-1.9.5p2-1.el8_9.
- tar-1.30-9.el8
- xz-5.2.4-4.el8_6
- zlib-1.2.11-25.el8

The vulnerability search was performed on 06/17/2024.

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 *Protection Profile for General Purpose Operating Systems*, Version 4.3, 27 September 2022 and *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019, 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 *Protection Profile for General Purpose Operating Systems*, Version 4.3, 27 September 2022 and *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019, 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 documentation referenced in Section 6 of this report. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated. Any additional customer documentation provided with the product, or that is available online, was not included in the scope of the evaluation and should not be relied upon when configuring or operating the device as evaluated.

The functionality evaluated is scoped exclusively to the security functional requirements specified in the ST. Other functionality included with the product, or within the operational environment, was not assessed as part of this evaluation and no further conclusions can be drawn about their effectiveness. This functionality and its impact on the product when deployed in the operational environment needs to be assessed separately in the context of the larger architecture that the product is a part of. No versions of the TOE models or Firmware versions, either earlier or later, were evaluated.

11 Annexes

Not applicable.

12 Security Target

[ST] CACI *Archon OS v3.0.0.2 Security Target*, Version 1.5, July 4, 2024.

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. *CACI Archon OS v3.0.0.2 Common Criteria User Guidance,* Version 1.2.
2. *CACI Archon OS v3.0.0.2 Security Target*, Version 1.5.
3. *Assurance Activity Report for CACI Archon OS v3.0.0.2*, v1.6.
4. *Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model*, Version 3.1 Revision 5.
5. *Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements*, Version 3.1 Revision 5.
6. *Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements*, Version 3.1 Revision 5.
7. *Common Evaluation Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 5.
8. *Equivalency Analysis for CACI Archon OS v3.0.0.2*, v2.2.
9. *Evaluation Technical Report for CACI Archon OS v3.0.0.2*, v1.4.
10. *Functional Package for Transport Layer Security (TLS)*, Version 1.1, 01 March 2019.
11. *Product Compliant List Entry, CACI Archon OS v3.0.0.2*
12. *Protection Profile for General Purpose Operating Systems*, Version 4.3, 27 September 2022.
13. *Test Report for CACI Archon OS v3.0.0.2 running on Dell Latitude 5410, Version 1.5*
14. *Test Report for CACI Archon OS v3.0.0.2 running on Dell Latitude 5430, Version 1.5*
15. *Validation Report for CACI Archon OS v3.0.0.2*
16. *Vulnerability Assessment for CACI Archon OS v3.0.0.2, v1.5*