National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

SpaceX Regulus

Report Number: CCEVS-VR-VID11327-2023

Dated: 08/07/2023

Version: 1.0

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

National Security Agency
ATTN:NIAP, Suite 6982
9800 Savage Road
Fort Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Fernando Guzman

Mike Quintos

Swapna Katikaneni

James Donndelinger

Common Criteria Testing Laboratory

Brandon Solberg

Brandon Mitchell

Shaunak Shah

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 SpaceX Regulus 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 August 2023. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for [CPP_ND_V2.2E] and [MOD_VPNGW_V1.1] .

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 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 [CPP_ND_V2.2E] and [MOD_VPNGW_V1.1]. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the SpaceX Regulus Security Target, Version 1.2, August 2023 and analysis performed by the Validation Team.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	SpaceX Regulus
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e [CPP_ND_V2.2E] PP-Module: PP-Module for Virtual Private Network (VPN) Gateways, Version 1.1 [MOD_VPNGW_V1.1]
Security Target	SpaceX Regulus Security Target
Evaluation Technical Report	Evaluation Technical Report for SpaceX Regulus version 1.0
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Space Exploration Technology Corp.
Developer	Space Exploration Technology Corp.
Common Criteria Testing Lab (CCTL)	Acumen Security Montgomery Village, MD
CCEVS Validators	Fernando Guzman Mike Quintos Swapna Katikaneni

	James Donndelinger

3 Architectural Information

The physical boundary of the TOE is the SpaceX Regulus chassis, which is a networked device providing connectivity to external networked entities. The TOE includes a specialized PCB board containing a Zynq Ultrascale+ ZU5 System on Chip (SoC) processor, based on Armv8-A Architecture, which executes the TOE software along with a NXP SE050F cryptographic accelerator. The TOE provides the following interfaces for management and network connectivity:

- 1x 100Mbps and 1x 10Gbps Ethernet ports for connectivity to trusted networks
- 1x 100Mbps, 1x 1Gbps, and 1x 10Gbps Ethernet ports for connectivity to untrusted networks
- UART for local serial console access
- 120VAC power input

4 Security Policy

The TOE provides the security functions required by the Collaborative Protection Profile for Network Devices, hereafter referred to as NDcPP v2.2e or NDcPP, along with the functionality specified in the PP-Module for VPN Gateways, or MOD_VPNGW 1.1.

4.1 Security Audit

The TOE generates audit events for all actions specified in Table 11 below and includes the identity of the entity that caused the event (if applicable), date and time of the event, event type, and outcome. Audit records are transmitted to an external log receiver via IPsec tunnels.

4.2 Cryptographic Support

The TOE implements CAVP validated cryptographic algorithms as specified in section 6.1 for asymmetric key generation, encryption/decryption, digital signatures, hashing, message authentication, and random bit generation. These algorithms are used to provide security for the SSH and IPsec connections, DRBG Operations, secure key generation and storage, digital signature operations, IPsec and SSH algorithm support, and digital signature operations.

4.3 Identification and Authentication

Identification and authentication are required both for user administrative access to the device and for establishing IPsec VPN peer connections.

User-level authentication is performed at the command line and supports remote and local access with pubkey authentication and passwords for SSH over the network and password authentication only for local console access. No management functionality is granted to users prior to this authentication process and all trusted passwords and SSH keys are stored locally on the TOE. Passwords must be a minimum length of 15 characters and only ECDSA P-384 keys are supported for pubkey authentication. If a user fails to authenticate via a password, their account will be automatically locked to remote access until an administrator-configurable amount of time has passed.

Authentication with an IPsec VPN peer is first established with IKEv2 based on X.509 ECDSA certificates. Peers that attempt to authenticate using certificates that are specified via CRLs will be rejected during the key exchange process. IPsec tunnels will not be established until the IKE process has been completed successfully for the full chain of trust.

4.4 Security Management

The security management functionality including access to cryptographic keys and TSF data is limited to the Security Administrator role. The TOE is managed via a remote SSH CLI and local serial CLI.

4.5 Packet Filtering

The TOE provides packet filtering and secure IPsec tunneling between the TOE and a trusted VPN endpoint.

4.6 Protection of the TOE Security Functionality (TSF)

The TOE prevents the reading of secret keys, private keys and passwords. During initial startup, the TOE runs a suite of self-tests to demonstrate correct operation of the cryptographic functionality. The TOE provides a means to verify firmware/software updates to the TOE using digital signature prior to installing those updates. The TOE provides reliable time stamps for itself.

4.7 TOE Access

The TOE terminates inactive remote and local sessions after an administrator configurable time-period. Sessions can also be terminated by the administrative user. The TOE also displays a configurable login banner prior to authenticating the user.

4.8 Trusted Path/Channels

The TOE provides a trusted path for administration via SSH. Trusted channels are implemented via IPsec to VPN endpoints as well as for audit log receivers.

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.

ID	Assumption
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 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 does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does 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. For vNDs, this assumption applies to the physical platform on which the VM runs.
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 a 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 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 and PP-Modules for particular types of Network Devices (e.g., firewall).

ID	Assumption
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 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. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
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.
A.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

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.

ID	Threat
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 tunnelling 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. a 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, 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

ID	Threat
	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 includes 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	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
T.DATA INTEGRITY	Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to modify the data without authorization. If known malicious external devices are able to communicate with devices on the protected network or if devices on the protected network can communicate with those external devices then the data contained within the communications may be susceptible to a loss of integrity.
T.NETWORK_ACCESS	Devices located outside the protected network may seek to exercise services located on the protected network that are intended to only be accessed from inside the protected network or only accessed by entities using an authenticated path into the protected network. Devices located outside the protected network may, likewise, offer services that are inappropriate for access from within the protected network. From an ingress perspective, VPN gateways can be configured so that only those network servers intended for external consumption by entities operating on a trusted network (e.g., machines operating on a network where the peer VPN gateways are supporting the connection) are accessible and only via the intended ports. This serves to mitigate the potential for network entities outside a protected network to access network servers or services intended only for consumption or access inside a protected network.

ID	Threat
	From an egress perspective, VPN gateways can be configured so that only specific external services (e.g., based on destination port) can be accessed from within a protected network, or moreover are accessed via an encrypted channel. For example, access to external mail services can be blocked to enforce corporate policies against accessing uncontrolled e-mail servers, or, that access to the mail server must be done over an encrypted link.
T.NETWORK_DISCLOSURE	Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If known malicious external devices are able to communicate with devices on the protected network, or if devices on the protected network can establish communications with those external devices (e.g., as a result of a phishing episode or by inadvertent responses to email messages), then those internal devices may be susceptible to the unauthorized disclosure of information. From an infiltration perspective, VPN gateways serve not only to limit access to only specific destination network addresses and ports within a protected network, but whether network traffic will be encrypted or transmitted in plaintext. With these limits, general network port scanning can be prevented from reaching protected networks or machines, and access to information on a protected network can be limited to that obtainable from specifically configured ports on identified network nodes (e.g., web pages from a designated corporate web server). Additionally, access can be limited to only specific source addresses and ports so that specific networks or network nodes can be blocked from accessing a protected network thereby further limiting the potential disclosure of information. From an exfiltration perspective, VPN gateways serve to limit how network nodes operating on a protected network can connect to and communicate with other networks limiting how and where they can disseminate information. Specific external networks can be blocked altogether or egress could be limited to specific addresses and/or ports. Alternately, egress options available to network nodes on a protected network can be carefully managed in order to, for example, ensure that outgoing connections are encrypted to further mitigate inappropriate disclosure of data through packet sniffing.
T.NETWORK_MISUSE	Devices located outside the protected network, while permitted to access particular public services offered inside the protected network, may attempt to conduct inappropriate activities while communicating with those

ID	Threat
	allowed public services. Certain services offered from within a protected network may also represent a risk when accessed from outside the protected network. From an ingress perspective, it is generally assumed that entities operating on external networks are not bound by the use policies for a given protected network. Nonetheless, VPN gateways can log policy violations that might indicate violation of publicized usage statements for publicly available services. From an egress perspective, VPN gateways can be configured to help enforce and monitor protected network use policies. As explained in the other threats, a VPN gateway can serve to limit dissemination of data, access to external servers, and even disruption of services – all of these could be related to the use policies of a protected network and as such are subject in some regards to enforcement. Additionally, VPN gateways can be configured to log network usages that cross between protected and external networks and as a result can serve to identify potential usage policy violations.
T.REPLAY_ATTACK	If an unauthorized individual successfully gains access to the system, the adversary may have the opportunity to conduct a "replay" attack. This method of attack allows the individual to capture packets traversing throughout the network and send the packets at a later time, possibly unknown by the intended receiver. Traffic is subject to replay if it meets the following conditions: ● Cleartext: an attacker with the ability to view unencrypted traffic can identify an appropriate segment of the communications to replay as well in order to cause the desired outcome. ● No integrity: alongside cleartext traffic, an attacker can make arbitrary modifications to captured traffic and replay it to cause the desired outcome if the recipient has no means to detect these.

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 [CPP_ND_V2.2E] and [MOD_VPNGW_V1.1].
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.

- Apart from the Admin Guide, additional customer documentation for the specific TOE was not included in the scope of the evaluation and therefore should not to be relied upon when configuring or operating the device as evaluated.
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.
- The following vulnerabilities were found not applicable to the TOE in the evaluated configuration as the only way to exploit the known vulnerabilities is if the TOE is out of the evaluated configuration or placed in an environment not suitable for the operation of the TOE given the assumptions in the protection profile.
    - CVE-2023-1079, CVE-2023-3923, CVE-2023-28866, CVE-2023-1513, CVE-2023-1252, CVE-2023-1249, CVE-2023-0590, CVE-2023-0386, CVE-2022-4095, CVE-2023-1281, CVE-2023-32269, CVE-2023-32233, CVE-2023-2513, CVE-2023-2124, CVE-2023-1859, CVE-2023-33203, CVE-2023-1195, CVE-2023-33288.

  However, the TOE administrator must be aware that the above vulnerabilities exist in the TOE and could be exploited if the attacker were to gain physical access to the TOE.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- SpaceX Regulus Security Target, v1.2
- Common Criteria Configuration Guide for Regulus VPN with SpaceX OS v1.0, v0.1

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

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

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The physical boundary of the TOE is the SpaceX Regulus chassis, which is a networked device providing connectivity to external networked entities. The TOE includes a specialized PCB board containing a Zynq Ultrascale+ ZU5 System on Chip (SoC) processor, based on Armv8-A Architecture, which executes the TOE software along with a NXP SE050F cryptographic accelerator. The TOE provides the following interfaces for management and network connectivity:

- 1x 100Mbps and 1x 10Gbps Ethernet ports for connectivity to trusted networks
- 1x 100Mbps, 1x 1Gbps, and 1x 10Gbps Ethernet ports for connectivity to untrusted networks
- UART for local serial console access
- 120VAC power input

7.2 Excluded Functionality

Any and all device functionality not explicitly covered by the SFRs in the Security Target were not tested during the course of the evaluation.

8 IT Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the proprietary Detailed Test Report for SpaceX Regulus, Version 1.2, July 25, 2023 (DTR), as summarized in the evaluation Assurance Activity Report (AAR).

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 [CPP_ND_V2.2E] and [MOD_VPNGW_V1.1]. The AAR, in sections 3 lists the tested devices, provides a list of test tools, and has diagrams of the test environment.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the SpaceX Regulus to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the SpaceX Regulus 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 [CPP_ND_V2.2E] and [MOD_VPNGW_V1.1].

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally the evaluator performed the Assurance Activities specified in the [CPP_ND_V2.2E] and [MOD_VPNGW_V1.1] related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of

the evaluation to ensure they were complete. Additionally the evaluator performed the Assurance Activities specified in the [CPP_ND_V2.2E] and [MOD_VPNGW_V1.1] related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the [CPP_ND_V2.2E] and [MOD_VPNGW_V1.1] and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validator reviewed the work of the evaluation team, and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the [CPP_ND_V2.2E] and [MOD_VPNGW_V1.1], 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. In compliance with AVA_VAN.1, the evaluator examined sources of publicly available information to identify potential vulnerabilities in the TOE. The sources of 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

- https://www.spacex.com/

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

- SpaceX
- Regulus
- Zynq Ultrascale+ ZU5
- Linux-based Operating System based on Kernel 5.15
- OpenIKED version 7.1
- OpenSSH version 8.9
- BoringSSL version 5416e4f16

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the [CPP_ND_V2.2E] and [MOD_VPNGW_V1.1], 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 [CPP_ND_V2.2E] and [MOD_VPNGW_V1.1], and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

As stated in section 5, the scope of this evaluation was limited to the functionality and assurances covered in the collaborative Protection Profile for Network Devices, Version 2.2e [CPP_ND_V2.2E] and PP-Module for Virtual Private Network (VPN) Gateways, Version 1.1 [MOD_VPNGW_V1.1]. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness. The evaluated configuration is dependent upon the TOE being configured per the evaluated configuration described in section 7 and the instructions in the Administrator Guide document listed in section 6.

11 Annexes

Not applicable.

12 Security Target

- SpaceX Regulus Security Target, v1.2 August 2023

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
5. Protection Profile for Network Devices, Version 2.2e [CPP_ND_V2.2E]
6. PP-Module for Virtual Private Network (VPN) Gateways, Version 1.1 [MOD_VPNGW_V1.1]
7. Proprietary Detailed Test Report for SpaceX Regulus, Version 1.2, July 25, 2023 (DTR).
8. Evaluation Technical Report for SpaceX Regulus – v1.1, August 2023(ETR)
9. Assurance Activity Report for SpaceX Regulus, Version 1.1, August 02, 2023(AAR).
10. Proprietary Vulnerability Assessment for SpaceX Regulus – v1.4, July 25, 2023(AVA)