Archon OS v3.0.0.2 Security Target

Version: 1.5

Date: July 4, 2024

CACI Inc.
44590 Guilford Dr
Ashburn, VA 20147
www.caci.com

Intertek Acumen Security, LLC
2400 Research Blvd, Suite 395
Rockville, MD 20850
www.acumensecurity.net

Revision History

Version	Date	Changes
Version 0.4	26 July, 2023	Initial Release
Version 0.5	3 August, 2023	Updates per vendor
Version 0.6	28 August, 2023	Updates per vendor
Version 0.7	31 August, 2023	Addressed QA review comments
Version 0.8	02 October, 2023	Applied TD0789
Version 0.9	14 November 2023	Addressing Validators comments
Version 1.0	07 December 2023	Addressing Validators comments
Version 1.1	April 22, 2024	Changed company name and evaluated TOE version
Version 1.2	May 26, 2024	Added CAVP certs Added and addressed TD0839
Version 1.3	June 1, 2024	Upgraded RHEL version to 8.10 and TOE version to 3.0.0.2. Removed NTP, automatic updates, and Firewall. Added App Note re ciphers to FCS_TLSC_EXT.1.1. Addressed Lead's comments
Version 1.4	June 8, 2024	Removed remote syslog.
Version 1.5	July 4, 2024	Addressed ECRs comments

Table of Contents

List of Tables

List of Figures

1 Introduction

The Security Target (ST) serves as the basis for the Common Criteria (CC) evaluation and identifies the Target of Evaluation (TOE), the scope of the evaluation, and the assumptions made throughout. This document will also describe the intended operational environment of the TOE, and the functional and assurance requirements that the TOE meets.

1.1 Security Target and TOE Reference

This section provides the information needed to identify and control the TOE and the ST.

Table 1 – TOE/ST Identification

Category	Identifier
ST Title	Archon OS v3.0.0.2 Security Target
ST Version	1.5
ST Date	July 4, 2024
ST Author	Intertek Acumen Security, LLC
TOE Identifier	Archon OS v3.0.0.2
TOE Version	v3.0.0.2
TOE Developer	CACI Inc,
Key Words	Operating System, TLS, Linux

1.2 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.

1.3 TOE Description

1.3.1 Type

The TOE is a general purpose operating system (OS), that supports multiple users, user permissions, access controls, and cryptographic functionality.

1.3.2 Evaluated Configuration

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

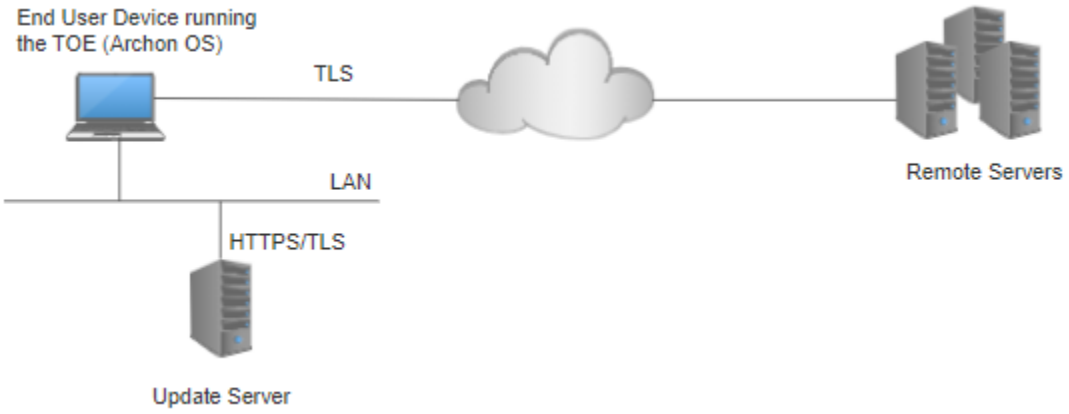
Table 2 – Archon OS v3.0.0.2 Hardware Platforms (EUDs)

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

1.3.3 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 running 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.

1.4 Logical Boundary

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).

1.4.1.1 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.

1.4.1.2 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 cryptographic library, and each cryptographic algorithm has been validated for conformance to the requirements specified in their respective standards as identified in Section 6.2 of this document.

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.

1.4.1.3 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.

1.4.1.4 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.

1.4.1.5 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.

1.4.1.6 TOE Access

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

1.4.1.7 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.

1.4.1.8 Trusted Path/Channels

The TOE supports TLSv1.2 to secure remote communications.

1.4.2 TOE Documentation

The following documents are essential to understanding and controlling the TOE in the evaluated configuration:

- [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*

1.5 Product Functionality not Included in the Scope of the Evaluation

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

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

2 Conformance Claims

2.1 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.

2.2 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

2.3 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 2.2 above.

2.3.1 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 4 – 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.

Technical Decision	Applicable (Y/N)	Exclusion Rationale (if applicable) and Notes
		Archives TD0727
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.

3 Security Problem Definition

The security problem description of this ST is taken directly from the claimed GPOS 4.3 PP ([PP_OS_4.3]) in Section 3 and is reproduced here for the convenience of the reader. The security problem is described in terms of the threats that the TOE is expected to address, assumptions about the operational environment, and any Organizational Security Policies (OSPs) that the TOE is expected to enforce. The Functional Package does not specify or augment the security problem definition.

3.1 Threats

The threats included in Table 5 are drawn directly from PP_OS_4.3.

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.

3.2 Assumptions

The assumptions included in Table 6 are drawn directly from the PP and Functional Packages.

Table 6 – 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.

ID	Description
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.

3.3 Organizational Security Policies

The PP and Functional Packages do not define any Organizational Security Policies (OSPs).

4 Security Objectives

The security objectives have been taken directly from the claimed GPOS 4.3 PP ([PP_OS_4.3]) and are reproduced here for the convenience of the reader. The Functional Packages do not specify any security objectives.

4.1 Security Objectives for the TOE

The security objectives in the following table apply to the TOE:

Table 7 – Security Objectives for the TOE

ID	Description
O.ACCOUNTABILITY	Conformant OSes ensure that information exists that allows administrators to discover unintentional issues with the configuration and operation of the operating system and discover its cause. Gathering event information and immediately transmitting it to another system can also enable incident response in the event of system compromise.
O.INTEGRITY	Conformant OSes ensure the integrity of their update packages. OSes are seldom if ever shipped without errors, and the ability to deploy patches and updates with integrity is critical to enterprise network security. Conformant OSes provide execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems.
O.MANAGMENT	To facilitate management by users and the enterprise, conformant OSes provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration and application execution control.
O.PROTECTED_STORAGE	To address the issue of loss of confidentiality of credentials in the event of loss of physical control of the storage medium, conformant OSes provide data-at-rest protection for credentials. Conformant OSes also provide access controls which allow users to keep their files private from other users of the same system.
O.PROTECTED_COMMS	To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant OSes provide mechanisms to create trusted channels for CSP and sensitive data. Both CSP and sensitive data should not be exposed outside of the platform.

4.2 Security Objectives for the Operational Environment

Security objectives for the operational environment assist the TOE in correctly providing its security functionality. These objectives, which are found in the table below, track with the assumptions about the TOE operational environment.

Table 8 – Security Objectives for the Operational Environment

ID	Description
OE.PLATFORM	The OS relies on being installed on trusted hardware.
OE.PROPER_USER	The user of the OS is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy. Standard user accounts are provisioned in accordance with the least privilege model. Users requiring higher levels of access should have a separate account dedicated for that use.
OE.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 Security Requirements

This section identifies the Security Functional Requirements (SFRs) for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1, Revision 5; the *Protection Profile for General Purpose Operating Systems*, Version 4.3; and the *Functional Package for Transport Layer Security (TLS), Version 1.1* and all international interpretations.

5.1 Extended Requirements

All the SFR and SAR extended requirements in this ST have been drawn from the *Protection Profile for General Purpose Operating Systems*, Version 4.3 and the *Functional Package for Transport Layer Security (TLS)*, Version 1.1. The PP_OS_V4.3 and the PKG_TLS_V1.1 define the extended SFRs. Since they have not been redefined in this ST, the PP_OS_V4.3 and the PKG_TLS_V1.1 should be consulted for more information regarding these extensions to CC Parts 2 and 3.

5.2 Conventions

The CC allows the following types of operations to be performed on the functional requirements: assignments, selections, refinements, and iterations. The following font conventions are used within this document to identify operations defined by CC:

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: Indicated by a slash followed by a descriptor for the purpose of the iteration. For example, FCS_HTTPS_EXT.1/Client indicates that the FCS_HTTPS_EXT.1 requirement applies specifically to HTTPS client functionality. SFR iterations are included in the PP and also defined by the ST author.
- The font formatting used in the PP, TDs, and Functional Package is retained except for information within brackets and strikethrough text. Operations within brackets use the conventions identified in the first three bullets above (italicized, bold, and underlined). Otherwise, if text within brackets does not include an operation, the text will be plain text (all non-italicized, non-underlined, and non-bold font). Strikethrough text has been deleted.

5.3 Security Functional Requirements

Table 9 – Security Functional Requirements

Requirement	Description
FAU_GEN.1	Audit Data Generation (Refined)
FCS_CKM.1	Cryptographic Key Generation (Refined)
FCS_CKM.2	Cryptographic Key Establishment (Refined)
FCS_CKM_EXT.4	Cryptographic Key Destruction
FCS_COP.1/ENCRYPT	Cryptographic Operation - Encryption/Decryption (Refined)
FCS_COP.1/HASH	Cryptographic Operation - Hashing (Refined)

Requirement	Description
FCS_COP.1/KEYHMAC	Cryptographic Operation - Keyed-Hash Message Authentication (Refined)
FCS_COP.1/SIGN	Cryptographic Operation - Signing (Refined)
FCS_RBG_EXT.1/KERN	Random Bit Generation (Kernel)
FCS_RBG_EXT.1/OSSL	Random Bit Generation (OpenSSL)
FCS_STO_EXT.1	Storage of Sensitive Data
FCS_TLS_EXT.1	TLS Protocol
FCS_TLSC_EXT.1	TLS Client Protocol
FCS_TLSC_EXT.2	TLS Client Support for Mutual Authentication
FCS_TLSC_EXT.4	Client Support for Renegotiation
FCS_TLSC_EXT.5	TLS Client Support for Supported Groups Extension
FDP_ACF_EXT.1	Access Controls for Protecting User Data
FIA_AFL.1	Authentication Failure Handling (Refined)
FIA_UAU.5	Multiple Authentication Mechanisms (Refined)
FIA_X509_EXT.1	X.509 Certificate Validation
FIA_X509_EXT.2	X.509 Certificate Authentication
FMT_MOF_EXT.1	Management of security functions behavior
FMT_SMF_EXT.1	Specification of Management Functions
FPT_ACF_EXT.1	Access controls
FPT_ASLR_EXT.1	Address Space Layout Randomization
FPT_SBOP_EXT.1	Stack Buffer Overflow Protection
FPT_SRP_EXT.1	Software Restriction Policies
FPT_TST_EXT.1	Boot Integrity
FPT_TUD_EXT.1	Trusted Update
FPT_TUD_EXT.2	Trusted Update for Application Software
FTA_TAB.1	Default TOE access banners
FTP_ITC_EXT.1	Trusted channel communication
FTP_TRP.1	Trusted Path

5.3.1 Audit Data Generation (FAU)

5.3.1.1 FAU_GEN.1 Audit Data Generation (Refined)

FAU_GEN.1.1 The **OS** shall be able to generate an audit record of the following auditable events:

a. Start-up and shut-down of the audit functions;

b. All auditable events for the [not specified] level of audit; and [

c.
- Authentication events (Success/Failure);
- Use of privileged/special rights events (Successful and unsuccessful security, audit, and configuration changes);
- Privilege or role escalation events (Success/Failure);
- [
  - File and object events (Successful and unsuccessful attempts to create, access, delete, modify, modify permissions),
  - User and Group management events (Successful and unsuccessful add, delete, modify, disable, enable, and credential change),
  - Audit and log data access events (Success/Failure),
  - Attempted application invocation with arguments (Success/Failure e.g. due to software restriction policy),
  - System reboot, restart, and shutdown events (Success/Failure),
  - Kernel module loading and unloading events (Success/Failure),
  - Administrator or root-level access events (Success/Failure),

  ]

].

FAU_GEN.1.2 The **OS** shall record within each audit record at least the following information:

a. Date and time of the event, type of event, subject identity (if applicable), and outcome (success or failure) of the event; and

b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

5.3.2 Cryptographic Support (FCS)

5.3.2.1 FCS_CKM.1 Cryptographic Key Generation (Refined)

FCS_CKM.1.1 The **OS** shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm [

- RSA schemes using cryptographic key sizes of 3072-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3,
- ECC schemes using "NIST curves" P-384 and [no other curves] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4,
- FFC Schemes using [safe primes that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes"]

].

Application Note: Applied TD0712.

5.3.2.2 FCS_CKM.2 Cryptographic Key Establishment (Refined)

FCS_CKM.2.1 The OS shall **implement functionality to perform cryptographic key establishment** in accordance with a specified cryptographic key **establishment** method: [

- Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography",
- Finite field-based key establishment schemes that meets NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"

].

5.3.2.3 FCS_CKM_EXT.4 Cryptographic Key Destruction

FCS_CKM_EXT.4.1 The OS shall destroy cryptographic keys and key material in accordance with a specified cryptographic key destruction method [

- For volatile memory, the destruction shall be executed by a [
  - single overwrite consisting of [zeroes],

  ],
- For non-volatile memory that consists of [
  - The invocation of an interface provided by the underlying platform that [
    - logically addresses the storage location of the key and performs a [*[administrator specified number (default of 3)]* overwrite consisting of [pseudo-random pattern]

  ]

]

].

FCS_CKM_EXT.4.2 The OS shall destroy all keys and key material when no longer needed.

5.3.2.4 FCS_COP.1/ENCRYPT Cryptographic Operation – Encryption/Decryption (Refined)

FCS_COP.1.1/ENCRYPT The **OS** shall perform [encryption/decryption services for data] in accordance with a specified cryptographic algorithm [

- AES-CBC (as defined in NIST SP 800-38A),

] and [

- AES-GCM (as defined in NIST SP 800-38D)

] and cryptographic key sizes 256-bit and [no other bit size].

Application Note: Applied TD0712.

5.3.2.5 FCS_COP.1/HASH Cryptographic Operation – Hashing (Refined)

FCS_COP.1.1/HASH The OS shall perform [cryptographic hashing services] in accordance with a specified cryptographic algorithm [

- SHA-256,
- SHA-384,

- SHA-512

] and message digest sizes [

- 256 bits,
- 384 bits,
- 512 bits

] that meet the following: [FIPS Pub 180-4].

Application Note: Applied TD0696.

5.3.2.6 FCS_COP.1/KEYHMAC Cryptographic Operation – Keyed-Hash Message Authentication (Refined)

FCS_COP.1.1/KEYHMAC The OS shall perform [keyed-hash message authentication services] in accordance with a specified cryptographic algorithm [

- SHA-256,
- SHA-384,
- SHA-512

] **with key sizes** [

- *256 bits,*
- *384 bits,*
- *512 bits*

] **and message digest** sizes [

- 256 bits,
- 384 bits,
- 512 bits

] that meet the following: [FIPS Pub 198-1 The Keyed-Hash Message Authentication Code and FIPS Pub 180-4 Secure Hash Standard].

Application Note: Applied TD0696.

5.3.2.7 FCS_COP.1/SIGN Cryptographic Operation – Signing (Refined)

FCS_COP.1.1/SIGN The **OS** shall perform [cryptographic signature services (generation and verification)] in accordance with a specified cryptographic algorithm [

- RSA schemes using cryptographic key sizes of [2048-bit (for secure boot only) or greater] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 4,
- ECDSA schemes using "NIST curves" P-384 and [no other curves] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5

].

Application Note: Applied TD0809.

5.3.2.8 FCS_RBG_EXT.1/KERN Random Bit Generation (Kernel)

FCS_RBG_EXT.1.1/KERN The OS shall perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using [

- HMAC_DRBG (any)

].

FCS_RBG_EXT.1.2/KERN The deterministic RBG used by the OS shall be seeded by an entropy source that accumulates entropy from a [

- platform-based noise source

] with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

Application Note: The KERN iteration applies to the Kernel API Cryptographic Library.

5.3.2.9 FCS_RBG_EXT.1/OSSL Random Bit Generation (OpenSSL)

FCS_RBG_EXT.1.1/OSSL The OS shall perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using [

- CTR_DRBG (AES)

].

FCS_RBG_EXT.1.2/OSSL The deterministic RBG used by the OS shall be seeded by an entropy source that accumulates entropy from a [

- platform-based noise source

] with a minimum of 256 bits of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

Application Note: The OSSL iteration applies to the OpenSSL Cryptographic module.

5.3.2.10 FCS_STO_EXT.1 Storage of Sensitive Data

FCS_STO_EXT.1.1 The OS shall implement functionality to encrypt sensitive data stored in non-volatile storage and provide interfaces to applications to invoke this functionality.

5.3.2.11 FCS_TLS_EXT.1 TLS Protocol

FCS_TLS_EXT.1.1 The product shall implement [

- TLS as a client

].

5.3.2.12 FCS_TLSC_EXT.1 TLS Client Protocol

FCS_TLSC_EXT.1.1 The product shall implement TLS 1.2 (RFC 5246) and [no earlier TLS versions] as a client that supports the cipher suites: [

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

] and also supports functionality for [

- mutual authentication,
- session renegotiation

].

FCS_TLSC_EXT.1.2 The product shall verify that the presented identifier matches the reference identifier according to RFC 6125.

FCS_TLSC_EXT.1.3 The product shall not establish a trusted channel if the server certificate is invalid [

- with no exceptions,

].

Application Note: Applied TD0442.

5.3.2.13 FCS_TLSC_EXT.2 TLS Client Support for Mutual Authentication

FCS_TLSC_EXT.2.1 The product shall support mutual authentication using X.509v3 certificates.

5.3.2.14 FCS_TLSC_EXT.4.1 Client Support for Renegotiation

FCS_TLSC_EXT.4.1 The product shall support secure renegotiation through use of the "renegotiation_info" TLS extension in accordance with RFC 5746.

5.3.2.15 FCS_TLSC_EXT.5 TLS Client Support for Supported Groups Extension

FCS_TLSC_EXT.5.1 The product shall present the Supported Groups Extension in the Client Hello with the following supported groups: [secp384r1].

5.3.3 User Data Protection (FDP)

5.3.3.1 FDP_ACF_EXT.1 Access Controls for Protecting User Data

FDP_ACF_EXT.1.1 The OS shall implement access controls which can prohibit unprivileged users from accessing files and directories owned by other users.

5.3.4 Identification and Authentication (FIA)

5.3.4.1 FIA_AFL.1 Authentication failure handling (Refined)

FIA_AFL.1.1 The **OS** shall detect when [

- an administrator configurable positive integer within *[1 – 65,535]*

] unsuccessful authentication attempts occur related to **events with** [

- authentication based on user name and password,

].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts for an account has been **met**, the **OS** shall: [Account Lockout].

Application Note: Applied TD0691.

5.3.4.2 FIA_UAU.5 Multiple Authentication Mechanisms (Refined)

FIA_UAU.5.1 The **OS** shall provide the following authentication mechanisms [

- authentication based on username and password,

] to support user authentication.

FIA_UAU.5.2 The **OS** shall authenticate any user's claimed identity according to the [*username and password: used at the local console. The TOE locally verifies the password hash matches the stored password hash associated with the provided username*].

5.3.4.3 FIA_X509.EXT.1 X.509 Certificate Validation

FIA_X509_EXT.1.1 The OS shall implement functionality to validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation
- The certificate path must terminate with a trusted CA certificate.
- The OS shall validate a certificate path by ensuring the presence of the basicConstraints extension, that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met.
- The TSF shall validate that any CA certificate includes "Certificate Signing" as a purpose the key usage field.
- The OS shall validate the revocation status of the certificate using [CRL as specified in RFC 8603] with [no exceptions]
- The OS shall validate the extendedKeyUsage field according to the following rules:
  - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing Purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
  - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
  - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the EKU field.
  - S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the EKU field.
  - OCSP certificates presented for OCSP responses shall have the OCSP Signing Purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the EKU field.
  - Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the EKU field.

Application Note: Applied TD0773.

FIA_X509_EXT.1.2 The OS shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

5.3.4.4 FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1 The OS shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [TLS, HTTPS] connections.

Application Note: Applied TD0789.

5.3.5 Security Management (FMT)

5.3.5.1 FMT_MOF_EXT.1 Management of Security Functions Behavior

FMT_MOF_EXT.1.1 The OS shall restrict the ability to perform the function indicated in the "Administrator" column in FMT_SMF_EXT.1.1 to the administrator.

Application Note: Applied TD0693.

5.3.5.2 FMT_SMF_EXT.1 Specification of Management Functions

FMT_SMF_EXT.1.1 The OS shall be capable of performing the following management functions:

Table 10 – Specification of Management Functions

Management Function	Administrator	User
1. Enable/disable [session timeout]	X	-
2. Configure [session] inactivity timeout	X	-
3. Import keys/secrets into the secure key storage.	X	-
4. Configure local audit storage capacity	X	-
5. Configure minimum password length	X	-
6. Configure minimum number of special characters in password	X	-
7. Configure minimum number of numeric characters in password	X	-
8. Configure minimum number of uppercase characters in password	X	-
9. Configure minimum number of lowercase characters in password	X	-
10. Configure lockout policy for unsuccessful authentication attempts through [timeouts between attempts]	X	-

Application Note: Applied TD0693.

5.3.6 Protection of the TSF (FPT)

5.3.6.1 FPT_ACF_EXT.1 Access Controls

FPT_ACF_EXT.1.1 The OS shall implement access controls which prohibit unprivileged users from modifying:

- Kernel and its drivers/modules
- Security audit logs
- Shared libraries
- System executables

- System configuration files
- [*no other objects*].

FPT_ACF_EXT.1.2 The OS shall implement access controls which prohibit unprivileged users from reading:

- Security audit logs
- System-wide credential repositories
- [*no other objects*].

5.3.6.2 FPT_ASLR_EXT.1 Address Space Layout Randomization

FPT_ASLR_EXT.1.1 The OS shall always randomize process address space memory locations with [*[at least 29]*] bits of entropy except for [*no exceptions*].

5.3.6.3 FPT_SBOP_EXT.1 Stack Buffer Overflow Protection

FPT_SBOP_EXT.1.1 The OS shall [employ stack-based buffer overflow protections].

5.3.6.4 FPT_SRP_EXT.1 Software Restriction Policies

FPT_SRP_EXT.1.1 The OS shall restrict execution to only programs which match an administrator-specified [

- file path,

].

5.3.6.5 FPT_TST_EXT.1 Boot Integrity

FPT_TST_EXT.1.1 The OS shall verify the integrity of the bootchain up through the OS kernel and [

- no other executable code

] prior to its execution through the use of [

- a digital signature using a hardware-protected asymmetric key

].

5.3.6.6 FPT_TUD_EXT.1 Trusted Update

FPT_TUD_EXT.1.1 The OS shall provide the ability to check for updates to the OS software itself and shall use a digital signature scheme specified in FCS_COP.1/SIGN to validate the authenticity of the response.

FPT_TUD_EXT.1.2 The OS shall [cryptographically verify] updates to itself using a digital signature prior to installation using schemes specified in FCS_COP.1/SIGN.

5.3.6.7 FPT_TUD_EXT.2 Trusted Update for Application Software

FPT_TUD_EXT.2.1 The OS shall provide the ability to check for updates to application software and shall use a digital signature scheme specified in FCS_COP.1/SIGN to validate the authenticity of the response.

FPT_TUD_EXT.2.2 The OS shall cryptographically verify the integrity of updates to applications using a digital signature specified by FCS_COP.1/SIGN prior to installation.

5.3.7 TOE Access (FTA)

5.3.7.1 FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1 Before establishing a user session, the OS shall display an advisory warning message regarding unauthorized use of the OS.

5.3.8 Trusted Path/Channels (FTP)

5.3.8.1 FTP_ITC_EXT.1 Trusted Channel Communication

FTP_ITC_EXT.1.1 The OS shall use [

- TLS as conforming to the Functional Package for Transport Layer Security (TLS), version 1.1 as a [client],

] and [no other protocols] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: [

- *[update server,*
- *user initiated TLS]*

] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

Application Note: Applied TD0789.

5.3.8.2 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 The **OS** shall provide a communication path between itself and [local] users that is logically distinct from other communication paths and provides assured

identification of its endpoints and protection of the communicated data from [modification, disclosure].

FTP_TRP.1.2 The **OS** shall permit [local users] to initiate communication via the trusted path.

FTP_TRP.1.3 The **OS** shall require use of the trusted path for [initial user authentication].

Application Note: Applied TD0839.

5.4 TOE SFR Dependencies Rationale for SFRs

PP_OS_V4.3 and PKG_TLS_V1.1 contain all the requirements claimed in this Security Target. As such, the dependencies are not applicable since the PP and Functional Package have been approved.

5.5 Security Assurance Requirements

The TOE assurance requirements for this ST are taken directly from the PP, derived from Common Criteria Version 3.1, Revision 5. The Functional Package for TLS does not define or require any additional SARs. The assurance requirements are summarized in Table 11.

Table 11 – Security Assurance Requirements

Assurance Class	Assurance Components	Component Description
Security Target	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security Objectives
	ASE_REQ.2	Derived Security Requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification
Development	ADV_FSP.1	Basic Functionality Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
Life Cycle Support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
	ALC_TSU_EXT.1	Timely Security Updates
Tests	ATE_IND.1	Independent Testing – Conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability Survey

5.6 Security Objectives Rationale

A mapping of the Security Functional Requirements taken from PP_OS_V4.3 to the Security Objectives for the TOE can be found in Section 4.1 of PP_OS_V4.3. This section also provides rationale for how SFRs satisfies the objective.

FCS_TLS_EXT.1 and FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.4, and FCS_TLSC_EXT.5 address O.PROTECTED_COMMS. The SFRs define the ability of the TOE to use the TLS protocol as a method of enforcing protected communications.

5.7 Rationale for Security Assurance Requirements

The Security Assurance Requirements were chosen because they are required by the PP_OS_V4.3, and the ST claims exact conformance to PP_OS_V4.3 and PKG_TLS_V1.1.

The functional specification describes the external interfaces of the TOE, such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.

6 TOE Summary Specification

This chapter identifies and describes how the Security Requirements identified above are met by the TOE.

Table 12 – TOE Summary Specification

Requirement	TSS Description
ALC_TSU_EXT.1	CACI provides a security update release for Archon OS at least once every 3 months. Resolution of vulnerabilities is expected within 180 days of public disclosure. For significant vulnerabilities, additional releases may be generated for quicker resolution. Archon OS vulnerabilities may be identified via internal testing, monitoring of CVE reports for Archon OS and third-party components, notification of vulnerabilities from third-party suppliers, or from customer reports. The CACI support team notifies customers of Archon OS vulnerabilities and informs them about resolutions. Because Archon OS is typically used on systems without internet access, it is expected that customers will download releases to their enterprise infrastructure and make it available to systems from one of their internal web servers. Customers are notified when releases are available, and provided with a URL for download. For vulnerabilities involving CACI-developed components, the CACI engineering team creates a Github ticket for each vulnerability to track the analysis and resolution of the issue. Issues are prioritized and worked to resolution, then incorporated into a product release. For vulnerabilities involving third-party components, CACI engineering works with the third-party supplier to ensure the vulnerability is known to them. The latest component fixes are continuously integrated into the Archon OS build cycle. This is particularly used with RHEL fixes, enabling Red Hat's efforts to be quickly integrated into Archon OS. Customers may report security issues related to Archon OS via the secure support portal at https://attilasec.zendesk.com/hc/en-us/requests/new [attilasec.zendesk.com].
FAU_GEN.1	The TOE generates and stores audit events using the Lightweight Audit Framework (LAF). The LAF is designed to be an audit system making the TOE 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 and forwards the events matching the filters to the audit daemon. Each audit record contains the date and time of event, type of event, subject identity, and the user identity if applicable. Access to audit data by normal users is prohibited by the DAC function of the TOE, which is used to restrict access to the audit trail and audit configuration files to the system administrator only.

Requirement	TSS Description

	An audit record consists of one or more lines of text containing fields in a “keyword=value” tagged format. The following information is contained in all audit record lines:
	• Type: indicates the source of the event, such as SYSCALL, PATH, USER_LOGIN, or LOGIN
	• Timestamp: Date and time (accurate to the millisecond) that the audit record was generated
	• Serial number: unique numerical event identifier appended to the timestamp.
	• Login ID (“auid”), the user ID of the user authenticated by the system (regardless if the user has changed his real and / or effective user ID afterwards)
	• Effective user and group ID: the effective user and group ID of the process at the time the audit event was generated.
	• Success or failure (where appropriate)
	• Process ID of the subject that caused the event (PID)
	• Hostname or terminal the subject used for performing the operation.
	• Information about the intended operation
	• The success or failure of the action
	This information is followed by event specific data. In some cases, such as SYSCALL event records involving file system objects, multiple text lines will be generated for a single event, these all have the same time stamp and serial number to permit easy correlation.
	The TOE is able to generate audit records for the following events:
	• Start-up and shut-down of the audit function
	• Authentication Events
	• Use of privileged/special rights events:
	  ○ Security, audit, and configuration changes
	  ○ Privilege or role escalation
	  ○ Administrator or root-level access events
	  ○ User and Group management
	• File and object events (create, access, delete, modify, modify permissions)
	• Audit and log data access events
	• Application invocation with arguments
	• System reboot, restart, and shutdown
	• Kernel module loading and unloading

FCS_CKM.1	The TOE implements RSA and ECC key generation and verification as specified in FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3 and B.4 (respectively). The TOE implements FFC key generation as specified in NIST SP 800-56A Revision 3, “Recommendation for Pair-Wise

Requirement	TSS Description
	Key Establishment Schemes". RSA key sizes of 3072 and 4096 are supported. ECC curve P-384 is supported. The FFC key size of L=3072 (Group 15) is supported. For more detail, refer to ST Section 6.2. The keys schemes usage is outlined in section 6.1.
FCS_CKM.2	For elliptic curve key establishment, the TOE implements Section 6.1.2.2 of NIST Special Publication 800-56A Revision 3. The TOE supports elliptic curve key establishment using the NIST curve P-384 during TLS mutual authentication when communicating with an update server. For Finite field key establishment, the TOE implements NIST Special Publication 800-56A Revision 3 . The TOE supports finite field key establishment using safe primes during TLS mutual authentication when communicating with remote servers.
FCS_CKM_EXT.4	For volatile memory, the TOE destroys keys and key material by performing a single overwrite consisting of zeroes. For non-volatile memory, the TOE destroys keys and key material by performing an administrator configurable number (default 3) of overwrites of the logical storage location with a pseudo random pattern. The pseudo random pattern is generated by an ISAAC PRNG which is initialized from /dev/urandom. See Section 6.1 for additional details of how each identified key is introduced into volatile and non-volatile memories. All instances of keys in non-volatile storage might not be deleted if the physical drive has replaced a sector containing a key with a spare sector. To minimize this risk, the physical drive should be end-of-life before a significant amount of damage to the drive's health can occur.
FCS_COP.1/ENCRYPT	The TOE implements AES as specified in FIPS 197 with 256-bit key sizes. The TOE implements the following modes: CBC and GCM.
FCS_COP.1/HASH	The TOE implements SHA-256, SHA-384, and SHA-512 as specified in FIPS 180-4. SHA-384 is used to verify the integrity of TOE updates and is used in TLS key establishment and key agreement. SHA-512 is used for the kernel DRBG, boot integrity (Secure Boot), and user password protection. SHA-256 is supported in the TOE in order to be compatible with remote systems (e.g. TLS servers, CAs) using RSA certificates that specify the use of SHA-256. RSA certificates are supported, and they specify a SHA value used with signatures associated with them. RSA certificates can be imported into the system as trusted CA certs for cert chains, and they can be received dynamically from TLS servers during connection setup.

Requirement	TSS Description
FCS_COP.1/KEYHMAC	The TOE implements HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 as specified in FIPS 198-1.
FCS_COP.1/SIGN	The TOE incorporates RSA and ECDSA signature generation and verification functionalities in accordance with the specifications outlined in FIPS 186-4, specifically in FIPS 186-4 Section 4 for RSA and FIPS 186-4 Section 5 for ECDSA. RSA key sizes of 2048 (for secure boot only), 3072, and 4096 are supported, utilizing SHA-256, SHA-384, and SHA-512 hashing algorithms. Additionally, ECDSA curve P-384 is supported, paired with SHA-384. For comprehensive information, please consult Section 6.2 of the Security Target.
FCS_RBG_EXT.1/OSSL FCS_RBG_EXT.1/KERN	The TOE offers two Deterministic Random Bit Generators (DRBGs), one in the kernel and the other in application space. The OpenSSL CTR_DRBG in application space receives a seed of at least 256 bits of entropy. This DRBG is utilized for generating session and ephemeral keys during TLS protocol negotiation, as well as for all other instances requiring entropy, such as nonce generation. The second DRBG is a kernel cryptographic API featuring an HMAC_DRBG (SHA-512) mechanism that receives a seed of at least 256 bits of entropy from the TOE's noise source. This particular DRBG is employed to produce random output for key generation and to supply seed material to the OpenSSL DRBG or TOE applications when invoked using /dev/random, /dev/urandom, or the 'getrandom' system call.
FCS_STO_EXT.1	The TOE includes the OpenSSL library to securely store sensitive data. OpenSSL provides file encryption services using AES-256 in CBC mode. Sensitive data is passwords and keys and can be found in the /etc directory which contains system-wide configuration files and system databases. Access to the files in /etc is limited with strict file permissions and/or encryption. Passwords are used for local user authentication. Keys are used in TLS key agreement and key establishment and signature verification.
FCS_TLS_EXT.1 FCS_TLSC_EXT.1 FCS_TLSC_EXT.2 FCS_TLSC_EXT.4 FCS_TLSC_EXT.5	The TOE provides a TLSv1.2 client implementation with the following ciphersuites: • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288, • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289, • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

Requirement	TSS Description
	The TOE presents the supported Elliptic Curves Extension in the Client Hello message with the P-384 curve (secp384r1). The TOE supports DH 15 for DHE key establishment. TOE establishes the reference identifier by parsing the DNS Name or IP address for the configured TLS server. The reference identifier is matched against the SAN, if present. If the SAN is not present, the referenced identifier is matched against the CN for DNS. For IP address, the TOE matches the identifier against the SAN only. The TOE supports wildcards in the DNS name of the server certificate (the left-most component in the presented certificate may be a wildcard (i.e. "*")). The TOE does not support URI reference identifiers, SRV reference identifiers, or certificate pinning. The TOE supports mutual authentication (MA). It will transmit its client certificate and engage in mutual authentication upon receiving the certificate request message from the server. Administrators are instructed in the TOE's guidance documentation in order to support MA, administrators must create a client certificate and store the certificate in the appropriate, protected directories. Administrators are also instructed how to configure the invocation of OpenSSL from HTTPS, CLI, and application programs to use the MA arguments in the OpenSSL call. Other than the MA configuration given in the administrator guidance, there is no other steps required to engage in MA. The TOE will not establish a trusted channel if the server certificate is invalid.
FDP_ACF_EXT.1	The TOE supports standard UNIX permission bits to provide one form of DAC. There are three sets of three bits that define access for three categories of users: the owning user, users in the owning group, and other users. The three bits in each set indicate the access permissions granted to each user category: one bit for read (r), one for write (w) and one for execute (x). Note that "write access" to file systems mounted as read only (e. g. CD-ROM) is always rejected (the exceptions are character and block device files which can still be written to as write operations do not modify the information on the storage media). The SAVETXT attribute is used for world-writable temp directories preventing the removal of files by users other than the owner. Each process has an inheritable "umask" attribute which is used to determine the default access permissions for new objects. It is a bit mask of the user/group/other read/write/execute bits and specifies the access bits to be removed from new objects. For example, setting the umask to "002" ensures that new objects will be writable by the owner and group, but not by others. The umask is defined by the administrator in the /etc/login.defs file or the value is "022" by default if not specified.

Requirement	TSS Description
	The TOE also provides support for POSIX type ACLs to define a fine-grained access control on a per-file or per-directory basis. An ACL entry contains the following information: • A tag type that specifies the type of the ACL entry • A qualifier that specifies an instance of an ACL entry type • A permission set that specifies the discretionary access rights for processes identified by the tag type and qualifier. An ACL contains exactly one entry of three different tag types (called the "required ACL entries" forming the "minimum ACL"). The standard UNIX file permission bits as described above are represented by the entries in the minimum ACL. A default ACL is an additional ACL which may be associated with a directory. This default ACL has no effect on the access to this directory. Instead, the default ACL is used to initialize the ACL for any file that is created in this directory. If the new file created is a directory it inherits the default ACL from its parent directory. When an object is created within a directory and the ACL is not defined with the function creating the object, the new object inherits the default ACL of its parent directory as its initial ACL. In addition, the following additional access control bits are processed by the kernel: • SUID bit: When an executable marked with the SUID bit is executed, the effective UID of the process is changed to the UID of the owner of the file. The SUID bit for file system objects other than files is ignored. • SGID bit: When an executable marked with the SGID bit is executed, the effective GID of the process is changed to the owning GID of the file. The SGID bit for file system objects other than files is ignored. • SAVETXT: When a directory is marked with the SAVETXT bit, only the owner of a file system object in that directory can remove it. This bit is commonly used for world-writable directories like /tmp. Only processes with the CAP_FOWNER capability are able to remove the file system object if their UID is different from the owning UID of the file system object. The TOE uses these permissions to protect the following from unauthorized modification: • Kernel, drivers, and kernel modules – files in: ○ /boot/ ○ /usr/lib/modules/ ○ /usr/lib/firmware/ • Security audit logs – files in:

Requirement	TSS Description
	○ /var/log/audit/ ○ /var/log/ • Shared libraries – files in: ○ /usr/lib64/ ○ /usr/lib/ • System executables – files in: ○ /usr/sbin/ ○ /usr/bin/ ○ /usr/libexec/ • System configuration files – files in: ○ /etc/ ○ /usr/lib/ Both shared libraries and configuration files are stored in /usr/lib/; however, all files in /usr/lib/ are protected from unauthorized modification, regardless of type.
FIA_AFL.1	The TOE will detect when an administrator configurable integer (`/etc/security/faillock.conf` file deny parameter) within 1-65,535 unsuccessful authentication attempts for authentication based on username and password occur related to password-based authentication at the local console. Once the specified number of unsuccessful authentication attempts for an account has been met, the TOE locks the account. Although it is possible to set the configured value to 0, that value would disable this function and the evaluated configuration requires the function to be enabled at all times.
FIA_UAU.5	The TOE supports authentication based on username and password at the local console. The TOE performs username and password authentication using a local set of credentials. During password-based login, a PAM (Pluggable Authentication Module) module is invoked which collects the username and password. The pam_unix module verifies the user is located in the password database file /etc/passwd and compares a hash (SHA-512) of the provided password with one previously stored in the file /etc/shadow. If successful, a user session is started. Otherwise, a delay occurs before allowing another attempt if permitted. The /etc/passwd file contains usernames, associated IDs, an indicator whether the password of the user is valid, the principal group id of the user and other (not security relevant) information. The /etc/shadow file contains a hash of the user's password, the user ID, the time the password was last changed, the expiration time, and the validity period of the

Requirement	TSS Description
	password. All data in the /etc/passwd directory are encrypted (AES-256 in CBC mode). Users are also warned to change their passwords at login time if the password expires soon and are prevented from logging in if the password has expired. The time of the last successful logins is recorded in the directory /var/log/faillock where one file per user is kept. Users can change their own password. Only administrators can add or delete users or change their properties.
FIA_X509_EXT.1 FIA_X509_EXT.2	The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS and HTTPS connections. The X.509 certificates are validated using the certificate path validation algorithm defined in RFC 5280, which can be summarized as follows: • the public key algorithm and parameters are checked. • the current date/time is checked against the validity period. • revocation status is checked using CRL. • issuer name of X matches the subject name of X+1. • extensions are processed. The certificate validity check is performed when the TOE receives the certificate during a TLS handshake. When the certificate being validated is for a TLS server, the TOE ensures the Extended Key Usage extension contains the Server Authentication purpose. The TOE ensures all CA certs contain the basic constraints extension and that the CA=TRUE flag is set. The TOE certificate validation algorithm also ensures that the certificate path terminates in a trusted root CA (i.e., a CA certificate configured on the TOE as trusted). If the validity check of a certificate fails, or if the TOE is unable to retrieve a valid and current CRL file from the CRL distribution point, the certificate is rejected. The TOE always verifies server certificates and always refuses to establish a trusted channel if the verification fails or if the TOE is unable to retrieve a valid and current CRL. There is not an override option.
FMT_MOF_EXT.1	The TOE restricts all “Administrator” management activities listed in FMT_SMF_EXT.1 to users who are members of the “wheel” group. The “wheel” group is a special user group used to control access to the super user (su) command. Members of this group are considered the administrators, because group membership allows users to elevate their

Requirement	TSS Description
	privileges, allowing management of the TOE, using the sudo command. The sudo command enables administrators to temporarily elevate their privileges without logging in as the root user.
FMT_SMF_EXT.1	The TOE allows the administrators to perform the following management activities: • Enable/disable session timeout. • Configure session timeout inactivity timeout. • Import keys/secrets into the secure key storage. • Configure local audit storage capacity. • Configure minimum password length. • Configure minimum number of special characters in password. • Configure minimum number of numeric characters in password. • Configure minimum number of uppercase characters in password. • Configure minimum number of lowercase characters in password. • Configure lockout policy for unsuccessful authentication attempts through timeouts between attempts. Non-administrative users are not allowed to manage the TOE.
FPT_ACF_EXT.1	The TOE uses the file/directory permissions described in FDP_ACF_EXT.1 to prevent unprivileged users from modifying: • Kernel and its drivers/modules • Security audit logs • Shared libraries • System executables • System configuration files
FPT_ASLR_EXT.1	The TOE executables are compiled as Position Independent Executables with the following amount of randomization: • exec 30 bits • heap 30 bits • so 29 bits • mmap 29 bits • stack 30 bits The TOE developer guidance instructs developers to compile non-TOE executables with PIE flags, so non-TOE executables have the same amount of randomization `-fpie-Wl,-pie`.
FPT_SBOP_EXT.1	The TOE is a stack-based OS and is compiled with the option “stack-protector-strong” to add a stack canary and associated verification code during the entry and exit of function frames to prevent stack-based buffer overflows.

Requirement	TSS Description
	The compiler guards functions that call “alloca”, or with buffers larger than or equal to 8 bytes, or those that have local array definitions, or have references to local frame addresses. Only variables that are actually allocated on the stack are considered. Optimized away variables or variables allocated in registers are not considered. The ST section 6.3 also lists all binaries not protected by stack mashing protections in use by the TOE, and their rationales for exclusion. The TOE does not store parameters/variables separately from control flow values.
FPT_SRP_EXT.1	The TOE includes a daemon, `fapolicyd`, that determines access rights to files based on a trust database and file or process attributes. By default, all applications that are packaged by rpm are automatically trusted. The user guidance provides instructions that enable the administrator to configure `fapolicyd`. The administrator is instructed to configure `fapolicyd` at TOE installation. Once configured, `fapolicyd` will create a file, `compiled.rules`, that identifies the trust/untrusted status of the files.

FPT_TST_EXT.1	The boot chain consists of the following steps:
	• Hardware responsibility
	  ○ Firmware initialization
	  ○ First stage boot loader (shim.efi)
	• TOE responsibility
	  ○ Second Stage Boot Loader (GRUB 2)
	  ○ First root filesystem (initramfs)
	  ○ Linux kernel (drivers and modules)
	
	Secure Boot is a UEFI firmware security feature developed by the UEFI Consortium that ensures only immutable and signed software is loaded during the boot time.
	
	The first application loaded by the platform’s firmware is the signed and trusted first-stage boot loader (shim.efi). This shim package itself holds the signing certificate and its own databases of trusted keys and hashes that are allowed to be loaded.
	
	The shim package’s signature is verified by the signing certificate’s RSA 2048 public key included in the shim package. The shim then uses this public key to verify the signature on the code signing public key held in the database. This code signing key is used to verify the signature of the second-stage boot loader, GRUB 2 (grubx64.efi).
	
	Next, GRUB 2 uses the code signing key to verify the signature on the first root filesystem (initramfs). Initramfs then uses RSA 4096 code (SHA 512) signing keys, from the database, to verify the signatures of the OS kernel.

Requirement	TSS Description
FPT_TUD_EXT.1 FPT_TUD_EXT.2	The TOE has the ability to check for updates to itself. Updates are verified by RSA 4096 with SHA-384 prior to installation. Updates to the TOE and application software are downloaded by the TOE from the Update Server.
FTA_TAB.1	The TOE can be configured to display an administrator configured advisory warning message prior to establishing a local or remote interactive user session.
FTP_ITC_EXT.1	The TOE provides a TLS Client protocol implementation which allows applications to protect communications with remote servers and protect secure software updates via the local repository using the TLS protocol.
FTP_TRP.1	The TOE provides a trusted path for local users. The TOE only supports local (keyboard) access which is considered a trusted interface. Protection of the data is reinforced by the FIA_AFL.1 requirement to authenticate users, ensuring only authorized users gain access.

6.1 Cryptographic Keys

Table 13 - Cryptographic Key and CSPs DetailsKeys	Type/Usage	Volatile Management Generator/Initiator	Non-Volatile Storage
TLS Diffie-Hellman Private Key	FFC Group 15 Or ECC P-384 used in TLS key agreement and key establishment.	Generated by the DRBG as specified by FCS_CKM.1 and FCS_CKM.2	N/A
TLS Pre-Master Secret	Data used to derive keys used in TLS key agreement and establishment.	Established using Diffie-Hellman (FFC & ECC)	N/A
TLS Session Keys	AES 256-bit and HMAC 384-bit used in HTTPS/TLS session encryption.	Derived from the TLS Pre-Master Secret	N/A
User Passwords	ASCII text	Entered by the user	Salted and hashed passwords are stored in /etc/shadow
File Encryption Key	AES 256-bit	Loaded from the filesystem, Or Entered by the user, Or Derived from a password entered by the user	N/A

6.2 CAVP Algorithm Certificate Details

Each of these cryptographic algorithms have been validated as identified in the table below:This section provides a table that lists all SFRs for which a CAVP certificate is claimed, the CAVP algorithm list name and the CAVP Certificate number.

Table 14: CAVP Certificates

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
FCS_CKM.1	RSA schemes using cryptographic key sizes of 3072-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3,	OpenSSL version 1.1.1k	RSA KeyGen (FIPS186-4)	A5342
	ECC schemes using "NIST curves" P-384 and [no other curves] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4,	OpenSSL version 1.1.1k	ECDSA KeyGen (FIPS186-4) ECDSA KeyVer (FIPS186-4)	A5342
	FFC Schemes using [safe primes that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes"]	OpenSSL version 1.1.1k	No CAVP certificate. Also, the evaluator confirmed that there is no assurance activity to be performed since "FIPS PUB 186-4" is not selected	
FCS_CKM.2	Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography",	OpenSSL version 1.1.1k	KAS-ECC-SSC SP800-56AR3	A5342
	Finite field-based key establishment schemes that meets NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"	OpenSSL version 1.1.1k	KAS-FFC-SSC SP800-56AR3	CCTL has performed all assurance /evaluation activities and documented in the ETR and AAR accordingly.

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
FCS_COP.1/ENCRYPT	AES-CBC (as defined in NIST SP 800-38A) and cryptographic key sizes [256-bit]	OpenSSL version 1.1.1k	AES-CBC	A5342
	AES-GCM (as defined in NIST SP 800-38D)] and cryptographic key sizes 256-bit and [no other bit size]	OpenSSL version 1.1.1k	AES-GCM	A5342
FCS_COP.1/SIGN	RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 4,	OpenSSL version 1.1.1k	RSA SigGen (FIPS186-4)	A5342
			RSA SigVer (FIPS186-4)	A5342
	ECDSA schemes using "NIST curves" P-384 and [no other curves] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5	OpenSSL version 1.1.1k	ECDSA SigGen (FIPS186-4)	A5342
			ECDSA SigVer (FIPS186-4)	A5342
FCS_COP.1/HASH	Cryptographic algorithm [SHA-256,SHA-384,SHA-512] and message digest sizes [• 256 bits, • 384 bits, • 512 bits] that meet the following: [FIPS Pub 180-4].	OpenSSL version 1.1.1k	SHA2-256 SHA2-384 SHA2-512	A5342
		Linux Kernel Crypto API	SHA2-512	A5343
FCS_COP.1/KEYHMAC	Cryptographic algorithm [SHA-256, SHA-384, SHA-512] with key sizes [*256 bits, 384 bits, 512 bits*] and	OpenSSL version 1.1.1k	HMAC-SHA2-256 HMAC-SHA2-384	A5342

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
	message digest sizes [• 256 bits, • 384 bits, • 512 bits] that meet the following: [FIPS Pub 198-1 The Keyed-Hash Message Authentication Code and FIPS Pub 180-4 Secure Hash Standard].		HMAC-SHA2-512	
		Linux Kernel Crypto API	HMAC-SHA2-512	A5343
FCS_RBG_EXT.1/OSSL	Random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using CTR_DRBG (AES)	OpenSSL version 1.1.1k	Counter DRBG	A5342
FCS_RBG_EXT.1/KERN	Random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using HMAC_DRBG (any)	Linux Kernel Crypto API	HMAC DRBG	A5343

6.3 Stack Smashing Protection

The TOE includes several binaries that were not compiled with stack-smashing protections enabled for a number of reasons. The reasons are listed below, followed by a list of binaries to which that reason applies.

glibc has special code for stack unwinding, exception handling, and another handwritten assembler. As such, it cannot enable the compiler-based stack protector. Refer to Appendix A for a list of files.

The following glibc files setup caches of information used application startup, so they are not invoked during normal application operations.

- /usr/sbin/*
  (except consoletype, findfs, fsfreeze, genhostid, grub2-set-bootflag, iconvconfig, ldconfig, load_policy, pivot_root, setcap, swaplabel, zdump, zic)

gcc has special handwritten assembler that establishes the C runtime environment before a program's main() function is invoked. As such, it cannot enable the compiler-based stack protector.

- /usr/lib/gcc/x86_64-redhat-linux/8/*
  (except libgcc.a:cpuinfo.o, libgcc.a:morestack.o, gcc-annobin.so.0.0.0)

gconv files are data tables used for character conversion. These do not contain executable code.

- /usr/lib64/gconv/*

(except libCNS.so, libGB.so, libISOIR165.so, libJIS.so, libJISX0213.so, libKSC.so)

This is part of the bootloader and has special needs during boot.

- /usr/lib/grub/i386-pc/kernel.exec

Firmware bundled with the OS is loaded onto various hardware devices and does not execute on the stack, so stack smashing protections are not needed.

- /usr/lib/firmware/*

7 Acronyms

Table 15 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ASLR	Address Space Layout Randomization
CBC	Cipher Block Chaining
CC	Common Criteria
CLI	Command Line Interface
CMC	Certificate Management over CMS
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EKU	Extended Key Usage
EST	Enrollment over Secure Transport
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
GPOS	General Purpose Operating System
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
NIAP	Nation Information Assurance Partnership
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OID	Object Identifier
OS	Operating System
OSP	Organizational Security Policy
PP	Protection Profile
RA	Registration Authority
RFC	Request for Comments
RHEL	Red Hat Enterprise Linux
RPM	Red Hat Packet Manager
RSA	Rivest, Shamir, & Adleman
SAR	Security Assurance Requirement

Acronym	Definition
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
S/MIME	Secure/Multi-purpose Internet Mail Extensions
ST	Security Target
SWID	Software Identification
TOE	Target of Evaluation
TLS	Transport Layer Security
TSS	TOE Summary Specification
LAF	Lightweight Audit Framework

Appendix A

context-filter.so, email-filter.so, nroff-filter.so, sgml-filter.so, tex-filter.so, texinfo-filter.so, sixaxis.so, libcolord_sensor_camera.so, libcolord_sensor_scanner.so, libcolord_sensor_argyll.so, libcolord_sensor_colorhug.so, libcolord_sensor_dtp94.so, libcolord_sensor_dummy.so, libcolord_sensor_huey.so, libdevmapper-event-lvm2mirror.so, libdevmapper-event-lvm2raid.so, libdevmapper-event-lvm2snapshot.so, libdevmapper-event-lvm2thin.so, libdevmapper-event-lvm2vdo.so, crocus_dri.so, iris_dri.so, kms_swrast_dri.so, nouveau_dri.so, r600_dri.so, radeonsi_dri.so, swrast_dri.so, virtio_gpu_dri.so, vmwgfx_dri.so, libcommon.so.12.1.0, libdynC_API.so.12.1.0, libdynDwarf.so.12.1.0, libdynElf.so.12.1.0, libdyninstAPI.so.12.1.0, libdyninstAPI_RT.so.12.1.0, libinstructionAPI.so.12.1.0, libparseAPI.so.12.1.0, libpatchAPI.so.12.1.0, libpcontrol.so.12.1.0, libstackwalk.so.12.1.0, libsymLite.so.12.1.0, libsymtabAPI.so.12.1.0, enchant_hunspell.so, afalg.so, capi.so, padlock.so, pkcs11.so, libedbus-private.so, libebookbackendfile.so, libebookbackendgoogle.so, libebookbackendldap.so, libebookbackendwebdav.so, libecalbackendcaldav.so, libecalbackendcontacts.so, libecalbackendfile.so, libecalbackendgtasks.so, libecalbackendhttp.so, libecalbackendweather.so, libcamelimapx.so, libcamellocal.so, libcamelnntp.so, libcamelpop3.so, libcamelsendmail.so, libcamelsmtp.so, module-credentials-goa.so, module-cache-reaper.so, module-gnome-online-accounts.so, module-google-backend.so, module-oauth2-services.so, module-outlook-backend.so, module-secret-monitor.so, module-trust-prompt.so, module-webdav-backend.so, module-yahoo-backend.so, libfu_plugin_acpi_dmar.so, libfu_plugin_acpi_facp.so, libfu_plugin_acpi_phat.so, libfu_plugin_amt.so, libfu_plugin_analogix.so, libfu_plugin_ata.so, libfu_plugin_bcm57xx.so, libfu_plugin_bios.so, libfu_plugin_ccgx.so, libfu_plugin_colorhug.so, libfu_plugin_cpu.so, libfu_plugin_cros_ec.so, libfu_plugin_dell.so, libfu_plugin_dell_dock.so, libfu_plugin_dell_esrt.so, libfu_plugin_dfu.so, libfu_plugin_dfu_csr.so, libfu_plugin_ebitdo.so, libfu_plugin_elanfp.so, libfu_plugin_elantp.so, libfu_plugin_emmc.so, libfu_plugin_ep963x.so, libfu_plugin_fastboot.so, libfu_plugin_fresco_pd.so, libfu_plugin_genesys.so, libfu_plugin_goodixmoc.so, libfu_plugin_hailuck.so, libfu_plugin_invalid.so, libfu_plugin_iommu.so, libfu_plugin_jabra.so, libfu_plugin_lenovo_thinklmi.so, libfu_plugin_linux_lockdown.so, libfu_plugin_linux_sleep.so, libfu_plugin_linux_swap.so, libfu_plugin_linux_tainted.so, libfu_plugin_logind.so, libfu_plugin_logitech_hidpp.so, libfu_plugin_msr.so, libfu_plugin_nitrokey.so, libfu_plugin_nordic_hid.so, libfu_plugin_nvme.so, libfu_plugin_optionrom.so, libfu_plugin_parade_lspcon.so, libfu_plugin_pci_bcr.so, libfu_plugin_pci_mei.so, libfu_plugin_pixart_rf.so, libfu_plugin_realtek_mst.so, libfu_plugin_redfish.so, libfu_plugin_rts54hid.so, libfu_plugin_rts54hub.so, libfu_plugin_scsi.so, libfu_plugin_steelseries.so, libfu_plugin_superio.so, libfu_plugin_synaptics_cape.so, libfu_plugin_synaptics_cxaudio.so, libfu_plugin_synaptics_mst.so, libfu_plugin_synaptics_prometheus.so, libfu_plugin_synaptics_rmi.so, libfu_plugin_system76_launch.so, libfu_plugin_test.so, libfu_plugin_thelio_io.so, libfu_plugin_thunderbolt.so, libfu_plugin_uefi_capsule.so, libfu_plugin_uefi_dbx.so, libfu_plugin_uefi_recovery.so, libfu_plugin_upower.so, libfu_plugin_usi_dock.so, libfu_plugin_vli.so, libfu_plugin_wacom_raw.so, libfu_plugin_wacom_usb.so, filefuncs.so, fnmatch.so, fork.so, inplace.so, intdiv.so, ordchr.so, readdir.so, readfile.so, revoutput.so, revtwoway.so, rwarray.so, time.so, libgconfbackend-oldxml.so, libgconfbackend-xml.so, libpixbufloader-ani.so, libpixbufloader-bmp.so, libpixbufloader-gif.so, libpixbufloader-icns.so, libpixbufloader-ico.so, libpixbufloader-jasper.so, libpixbufloader-jpeg.so, libpixbufloader-pnm.so, libpixbufloader-qtif.so, libpixbufloader-svg.so, libpixbufloader-tga.so, libpixbufloader-tiff.so, libpixbufloader-xbm.so, libpixbufloader-xpm.so, cldr-plurals, hostname, urlget, libdconfsettings.so, libgiognomeproxy.so, libgiognutls.so, libgiolibproxy.so, libgsettingsgconfbackend.so, libgimarshallingtests.so, libregress.so, libwarnlib.so, gkm-gnome2-store-standalone.so, gkm-secret-store-standalone.so, gkm-ssh-store-standalone.so, gkm-xdg-store-

standalone.so, libgsd.so, libgnome-shell-menu.so, libgnome-shell.so, libgvc.so, libst-1.0.so, libgoawebextension.so, libgst1394.so, libgstadder.so, libgstalaw.so, libgstalpha.so, libgstalphacolor.so, libgstalsa.so, libgstapetag.so, libgstapp.so, libgstaudioconvert.so, libgstaudiofx.so, libgstaudiomixer.so, libgstaudioparsers.so, libgstaudiorate.so, libgstaudioresample.so, libgstaudiotestsrc.so, libgstauparse.so, libgstautodetect.so, libgstavi.so, libgstcairo.so, libgstcompositor.so, libgstcoreelements.so, libgstcoretracers.so, libgstcutter.so, libgstdebug.so, libgstdeinterlace.so, libgstdtmf.so, libgstdv.so, libgsteffectv.so, libgstencoding.so, libgstequalizer.so, libgstflac.so, libgstflv.so, libgstflxdec.so, libgstgdkpixbuf.so, libgstgio.so, libgstgoom.so, libgstgoom2k1.so, libgsticydemux.so, libgstid3demux.so, libgstimagefreeze.so, libgstinterleave.so, libgstisomp4.so, libgstjpeg.so, libgstlame.so, libgstlevel.so, libgstlibvisual.so, libgstmatroska.so, libgstmpg123.so, libgstmulaw.so, libgstmultifile.so, libgstmultipart.so, libgstnavigationtest.so, libgstogg.so, libgstopengl.so, libgstopus.so, libgstoss4.so, libgstossaudio.so, libgstoverlaycomposition.so, libgstpango.so, libgstpbtypes.so, libgstplayback.so, libgstpng.so, libgstpulseaudio.so, libgstrawparse.so, libgstreplaygain.so, libgstrtp.so, libgstrtpmanager.so, libgstrtsp.so, libgstshapewipe.so, libgstshout2.so, libgstsmpte.so, libgstsoup.so, libgstspectrum.so, libgstspeex.so, libgstsubparse.so, libgsttaglib.so, libgsttcp.so, libgsttheora.so, libgsttwolame.so, libgsttypefindfunctions.so, libgstudp.so, libgstvideo4linux2.so, libgstvideobox.so, libgstvideoconvert.so, libgstvideocrop.so, libgstvideofilter.so, libgstvideomixer.so, libgstvideorate.so, libgstvideoscale.so, libgstvideotestsrc.so, libgstvolume.so, libgstvorbis.so, libgstvpx.so, libgstwavenc.so, libgstwavpack.so, libgstwavparse.so, libgstximagesink.so, libgstximagesrc.so, libgstxvimagesink.so, libgsty4menc.so, libadwaita.so, libpixmap.so, im-ibus.so, libprintbackend-cups.so, libprintbackend-file.so, libprintbackend-lpr.so, libatk-bridge.so, libferret.so, libgail.so, libprintbackend-cloudprint.so, libcanberra-gtk3-module.so, spake.so, k5tls.so, libldb-key-value.so, libldb-mdb-int.so, libldb-tdb-err-map.so, libldb-tdb-int.so, asq.so, ldap.so, ldb.so, mdb.so, paged_searches.so, rdn_name.so, sample.so, server_sort.so, skel.so, tdb.so, libaccountsservice.so.0.0.0, libacl.so.1.1.2253, libaio.so.1.0.0, libaio.so.1.0.1, libanl-2.28.so, libannocheck.so.0.0.0, libarchive.so.13.3.3, libasm-0.188.so, libasound.so.2.0.0, libaspell.so.15.1.5, libasprintf.so.0.0.0, libassuan.so.0.8.1, libasyncns.so.0.3.1, libatasmart.so.4.0.5, libatk-1.0.so.0.22810.1, libatk-bridge-2.0.so.0.0.0, libatomic_ops_gpl.so.1.1.2, libatomic_ops.so.1.1.1, libatopology.so.2.0.0, libatspi.so.0.0.1, libattr.so.1.1.2448, libaudit.so.1.0.0, libauparse.so.0.0.0, libauthselect.so.3.1.1, libavahi-client.so.3.2.9, libavahi-common.so.3.5.3, libavahi-glib.so.1.0.2, libavc1394.so.0.3.0, libbabeltrace-ctf-metadata.so.1.0.0, libbabeltrace-ctf.so.1.0.0, libbabeltrace-ctf-text.so.1.0.0, libbabeltrace-dummy.so.1.0.0, libbabeltrace-lttng-live.so.1.0.0, libbabeltrace.so.1.0.0, libbd_crypto.so.2.0.0, libbd_fs.so.2.0.0, libbd_loop.so.2.0.0, libbd_mdraid.so.2.0.0, libbd_part_err.so.2.0.0, libbd_part.so.2.0.0, libbd_swap.so.2.0.0, libbd_utils.so.2.1.0, libbfd-2.30-119.el8.so, libblkid.so.1.1.0, libblockdev.so.2.0.0, libbluetooth.so.3.19.6, libboost_atomic.so.1.66.0, libboost_chrono.so.1.66.0, libboost_date_time.so.1.66.0, libboost_filesystem.so.1.66.0, libboost_system.so.1.66.0, libboost_thread.so.1.66.0, libboost_timer.so.1.66.0, libbrotlicommon.so.1.0.6, libbrotlidec.so.1.0.6, libbrotlienc.so.1.0.6, libbytesize.so.1.0.0, libbz2.so.1.0.6, libc-2.28.so, libcairo-gobject.so.2.11512.0, libcairo-script-interpreter.so.2.11512.0, libcairo.so.2.11512.0, libcamel-1.2.so.61.0.0, libcanberra-alsa.so, libcanberra-gstreamer.so, libcanberra-multi.so, libcanberra-null.so, libcanberra-pulse.so, libcanberra-gtk3.so.0.1.9, libcanberra.so.0.2.5, libcap-ng.so.0.0.0, libcap.so.2.48, libcheese-gtk.so.25.1.0, libcheese.so.8.0.10, libclutter-1.0.so.0.2600.2, libclutter-gst-3.0.so.0.26.0, libclutter-gtk-1.0.so.0.800.4, libcogl-pango.so.20.4.2, libcogl-path.so.20.4.2, libcogl.so.20.4.2, libcolord-gtk.so.1.0.3, libcolordprivate.so.2.0.5, libcolord.so.2.0.5, libcolorhug.so.2.0.5, libcom_err.so.2.1, libcomps.so.0, libcord.so.1.3.0, libcrack.so.2.9.0, libcroco-0.6.so.3.0.1, libcrypto.so.1.1.1k, libcryptsetup.so.12.6.0, libcrypt.so.1.1.0, libcupscgi.so.1, libcupsimage.so.2, libcupsmime.so.1, libcupsppdc.so.1, libcups.so.2, libcurl.so.4.5.0, libdatrie.so.1.3.2, libdb-5.3.so, libdbus-1.so.3.19.7, libdbus-glib-1.so.2.3.4, libdcerpc-binding.so.0.0.1,

libdcerpc-server-core.so.0.0.1, libdcerpc.so.0.0.1, libdconf.so.1.0.0, libdebuginfod-0.188.so, libdevmapper-event-lvm2.so.2.03, libdevmapper-event.so.1.02, libdevmapper.so.1.02, libdl-2.28.so, product-id.so, libdnf.so.2, libdrm_amdgpu.so.1.0.0, libdrm_intel.so.1.0.0, libdrm_nouveau.so.2.0.0, libdrm_radeon.so.1.0.1, libdrm.so.2.4.0, libdv.so.4.0.3, libdw-0.188.so, libe2p.so.2.3, libebackend-1.2.so.10.0.0, libebook-1.2.so.19.1.3, libebook-contacts-1.2.so.2.0.0, libecal-1.2.so.19.0.0, libedata-book-1.2.so.25.0.0, libedata-cal-1.2.so.28.0.0, libedataserver-1.2.so.23.0.0, libedataserverui-1.2.so.2.0.0, libedit.so.0.0.56, libefa.so.1.2.44.0, libefiboot.so.1.37, libefivar.so.1.37, libEGL_mesa.so.0.0.0, libEGL.so.1.1.0, libelf-0.188.so, libenchant-2.so.2.2.3, libepoxy.so.0.0.0, libestr.so.0.0.0, libevdev.so.2.3.0, libevent-2.1.so.6.0.2, libevent_core-2.1.so.6.0.2, libevent_extra-2.1.so.6.0.2, libevent_openssl-2.1.so.6.0.2, libevent_pthreads-2.1.so.6.0.2, libexpat.so.1.6.7, libexslt.so.0.8.20, libext2fs.so.2.4, libfastjson.so.4.3.0, libfdisk.so.1.1.0, libffi.so.6.0.2, libFLAC++.so.6.3.0, libFLAC.so.8.3.0, libfontconfig.so.1.12.0, libfontenc.so.1.0.0, libform.so.6.1, libformw.so.6.1, libfreebl3.so, libfreeblpriv3.so, libfreetype.so.6.16.1, libfribidi.so.0.4.0, libfuse3.so.3.3.0, libfuse.so.2.9.7, libfwupdplugin.so.5.0.0, libfwupd.so.2.0.0, libgailutil-3.so.0.0.0, libgailutil.so.18.0.1, libgbm.so.1.0.0, libgcab-1.0.so.0.0.0, libgccpp.so.1.3.1, libgck-1.so.0.0.0, libgconf-2.so.4.1.5, libgcr-base-3.so.1.0.0, libgcr-ui-3.so.1.0.0, libgcrypt.so.20.2.5, libgc.so.1.3.2, libgdata.so.22.3.0, libgdbm_compat.so.4.0.0, libgdbm.so.6.0.0, libgdk-3.so.0.2200.30, libgdk_pixbuf-2.0.so.0.3612.0, libgdk-x11-2.0.so.0.2400.32, libgdm.so.1.0.0, libgeoclue-2.so.0.0.0, libgeocode-glib.so.0.0.0, libgettextlib-0.19.8.1.so, libgettextpo.so.0.5.4, libgettextsrc-0.19.8.1.so, libgio-2.0.so.0.5600.4, libgirepository-1.0.so.1.0.0, libgjs.so.0.0.0, libglapi.so.0.0.0, libGLdispatch.so.0.0.0, libGLESv1_CM.so.1.2.0, libGLESv2.so.2.1.0, libglib-2.0.so.0.5600.4, libGL.so.1.7.0, libGLX_mesa.so.0.0.0, libGLX.so.0.0.0, libgmodule-2.0.so.0.5600.4, libgmp.so.10.3.2, libgnome-bluetooth.so.13.0.2, libgnome-desktop-3.so.17.0.6, libgnomekbd.so.8.0.0, libgnomekbdui.so.8.0.0, libgnutls-dane.so.0.4.1, libgnutls.so.30.28.2, libgoa-1.0.so.0.0.0, libgoa-backend-1.0.so.1.0.0, libgobject-2.0.so.0.5600.4, libgomp.so.1.0.0, libgpg-error.so.0.24.2, libgpgme.so.11.22.1, libgraphite2.so.3.0.1, libgrilo-0.3.so.0.306.1, libgrlnet-0.3.so.0.306.0, libgrlpls-0.3.so.0.306.0, libgsm.so.1.0.17, libgssapi_krb5.so.2.2, libgssrpc.so.4.2, libgstallocators-1.0.so.0.1601.0, libgstapp-1.0.so.0.1601.0, libgstaudio-1.0.so.0.1601.0, libgstbase-1.0.so.0.1601.0, libgstcheck-1.0.so.0.1601.0, libgstcontroller-1.0.so.0.1601.0, libgstfft-1.0.so.0.1601.0, libgstgl-1.0.so.0.1601.0, libgstnet-1.0.so.0.1601.0, libgstpbutils-1.0.so.0.1601.0, libgstreamer-1.0.so.0.1601.0, libgstriff-1.0.so.0.1601.0, libgstrtp-1.0.so.0.1601.0, libgstrtsp-1.0.so.0.1601.0, libgstsdp-1.0.so.0.1601.0, libgsttag-1.0.so.0.1601.0, libgstvideo-1.0.so.0.1601.0, libgthread-2.0.so.0.5600.4, libgtk-3.so.0.2200.30, libgtk-x11-2.0.so.0.2400.32, libgtop-2.0.so.11.0.0, libgudev-1.0.so.0.2.0, libguile-2.0.so.22.8.1, libguilereadline-v-18.so.18.0.0, libgusb.so.2.0.10, libgweather-3.so.15.0.0, libhandle.so.1.0.3, libharfbuzz-icu.so.0.10705.0, libharfbuzz.so.0.10705.0, libhistory.so.7.0, libhogweed.so.4.5, libhunspell-1.6.so.0.0.1, libhyphen.so.0.3.0, libibus-1.0.so.5.0.519, libbnxt_re-rdmav34.so, libcxgb4-rdmav34.so, libhfi1verbs-rdmav34.so, libhns-rdmav34.so, libirdma-rdmav34.so, libqedr-rdmav34.so, librxe-rdmav34.so, libsiw-rdmav34.so, libvmw_pvrdma-rdmav34.so, libibverbs.so.1.14.44.0, libical_cxx.so.3.0.3, libical.so.3.0.3, libicalss_cxx.so.3.0.3, libicalss.so.3.0.3, libicalvcal.so.3.0.3, libICE.so.6.3.0, libicudata.so.60.3, libicui18n.so.60.3, libicuio.so.60.3, libicutest.so.60.3, libicutu.so.60.3, libicuuc.so.60.3, libidn2.so.0.3.6, libiec61883.so.0.1.1, libimaevm.so.2.0.0, libimobiledevice.so.6.0.0, libinput.so.10.13.0, libIntelXvMC.so.1.0.0, libip4tc.so.0.1.0, libip4tc.so.2.0.0, libip6tc.so.0.1.0, libip6tc.so.2.0.0, libipset.so.13.1.0, libipt.so.1.6.1, libirml.so.1, libisl.so.13.1.0, libisl.so.15.1.1, libjansson.so.4.14.0, libjasper.so.4.0.0, libjavascriptcoregtk-4.0.so.18.21.8, libjbig85.so.2.1, libjbig.so.2.1, libjcat.so.1.0.0, libjose.so.0.0.0, libjpeg.so.62.2.0, libjq.so.1.0.4, libjson-c.so.4.0.0, libjson-glib-1.0.so.0.400.4, libk5crypto.so.3.1, libkcapi.so.1.2.0, libkdb5.so.10.0, libkeyutils.so.1.6, libkmod.so.2.3.3, libkrad.so.0.0, libkrb5.so.3.3, libkrb5support.so.0.1, libksba.so.8.11.6, liblber-2.4.so.2.10.9, liblcms2.so.2.0.8, libldap-2.4.so.2.10.9, libldap_r-2.4.so.2.10.9, libldb.so.2.6.1, libldns.so.2.0.0, libLLVM-15.so, liblmdb.so.0.0.0,

libltdl.so.7.3.1, libLTO.so.15, liblua-5.3.so, libluksmeta.so.0.0.0, liblvm2cmd.so.2.03, liblz4.so.1.8.3, liblzma.so.5.2.4, libm-2.28.so, libmagic.so.1.0.0, libmbim-glib.so.4.7.0, libmcpp.so.0.3.0, libmenu.so.6.1, libmenuw.so.6.1, libmlx4.so.1.0.44.0, libmlx5.so.1.24.44.0, libmm-glib.so.0.9.0, libmnl.so.0.2.0, libmodman.so.1.0.0, libmodulemd.so.2.13.0, libmount.so.1.1.0, libmozjs-60.so.0.0.0, libmp3lame.so.0.0.0, libmpc.so.3.1.0, libmpfr.so.4.1.6, libmpg123.so.0.44.8, libmtdev.so.1.0.0, libmutter-4.so.0.0.0, libmvec-2.28.so, libncurses.so.6.1, libncursesw.so.6.1, libndp.so.0.1.1, libndr-krb5pac.so.0.0.1, libndr-nbt.so.0.0.1, libndr.so.3.0.0, libndr-standard.so.0.0.1, libnetfilter_conntrack.so.3.6.0, libnet.so.1.7.0, libnettle.so.6.5, libnfnetlink.so.0.2.0, libnftables.so.1.0.0, libnftnl.so.11.2.0, libnghttp2.so.14.17.0, libnl-3.so.200.26.0, libnl-genl-3.so.200.26.0, libnl-idiag-3.so.200.26.0, libnl-nf-3.so.200.26.0, libnl-route-3.so.200.26.0, libnl-xfrm-3.so.200.26.0, libnma.so.0.0.0, libnm.so.0.1.0, libnotify.so.4.0.0, libnpth.so.0.1.1, libnsl.so.2.0.0, libnspr4.so, libnss3.so, libnss_altfiles.so.2, libnss_compat-2.28.so, libnssdbm3.so, libnss_dns-2.28.so, libnss_files-2.28.so, libnss_myhostname.so.2, libnss_resolve.so.2, libnsssysinit.so, libnss_systemd.so.2, libnssutil3.so, liboauth.so.0.8.7, libogg.so.0.8.2, libonig.so.5.0.0, libopcodes-2.30-119.el8.so, libOpenGL.so.0.0.0, libopenjp2.so.2.4.0, libopenscap.so.25.5.1, libopts.so.25.16.1, libopus.so.0.6.1, liborc-0.4.so.0.28.0, liborc-test-0.4.so.0.28.0, libostree-1.so.1.0.0, libout123.so.0.2.2, libp11-kit.so.0.3.0, libp11.so.3.4.2, libpamc.so.0.82.1, libpam_misc.so.0.82.1, libpam.so.0.84.2, libpanel.so.6.1, libpanelw.so.6.1, libpango-1.0.so.0.4200.3, libpangocairo-1.0.so.0.4200.3, libpangoft2-1.0.so.0.4200.3, libpangoxft-1.0.so.0.4200.3, libparted-fs-resize.so.0.0.1, libparted.so.2.0.1, libpcap.so.1.9.1, libpciaccess.so.0.11.1, libpcre2-16.so.0.7.1, libpcre2-8.so.0.7.1, libpcre2-posix.so.2.0.1, libpcreposix.so.0.0.6, libpcre.so.1.2.10, libperl.so.5.26.3, libpipeline.so.1.5.0, libpipewire-0.3.so.0.306.0, libpixman-1.so.0.38.4, libpkgconf.so.3.0.0, libplc4.so, libplds4.so, libplist++.so.3.1.0, libplist.so.3.1.0, libply-boot-client.so.5.0.0, libply.so.5.0.0, libply-splash-core.so.5.0.0, libply-splash-graphics.so.5.0.0, libpng16.so.16.34.0, libpolkit-agent-1.so.0.0.0, libpolkit-gobject-1.so.0.0.0, libpopt.so.0.0.1, libprocps.so.7.1.0, libprotobuf-c.so.1.0.0, libprotobuf.so.15.0.0, libproxy.so.1.0.0, libpsl.so.5.3.1, libpspell.so.15.1.5, libpsx.so.2.48, libpulse-mainloop-glib.so.0.0.6, libpulse-simple.so.0.1.1, libpulse.so.0.23.0, libpwquality.so.1.0.2, libpython3.6m.so.1.0, libqb.so.0.19.0, libqmi-glib.so.5.9.0, libQt5Concurrent.so.5.15.3, libQt5Core.so.5.15.3, libQt5DBus.so.5.15.3, libQt5EglFSDeviceIntegration.so.5.15.3, libQt5EglFsKmsSupport.so.5.15.3, libQt5Gui.so.5.15.3, libQt5Network.so.5.15.3, libQt5OpenGL.so.5.15.3, libQt5PrintSupport.so.5.15.3, libQt5QmlModels.so.5.15.3, libQt5Qml.so.5.15.3, libQt5QmlWorkerScript.so.5.15.3, libQt5QuickParticles.so.5.15.3, libQt5QuickShapes.so.5.15.3, libQt5Quick.so.5.15.3, libQt5QuickTest.so.5.15.3, libQt5QuickWidgets.so.5.15.3, libQt5Sql.so.5.15.3, libQt5Test.so.5.15.3, libQt5Widgets.so.5.15.3, libQt5XcbQpa.so.5.15.3, libQt5XmlPatterns.so.5.15.3, libQt5Xml.so.5.15.3, libquvi-0.9-0.9.4.so, libraw1394.so.11.1.0, libreadline.so.7.0, libRemarks.so.15, librepo.so.0, librest-0.7.so.0.0.0, librest-extras-0.7.so.0.0.0, librhsm.so.0, librom1394.so.0.3.0, librpmbuild.so.8.2.0, librpmio.so.8.2.0, librpmostree-1.so.1.0.0, librpmsign.so.8.2.0, librpm.so.8.2.0, librsvg-2.so.2.42.7, librt-2.28.so, libsamba-credentials.so.1.0.0, libsamba-errors.so.1.0.0, libsamba-hostconfig.so.0.0.1, libsamba-passdb.so.0.28.0, libsamba-util.so.0.0.1, libsamdb.so.0.0.1, libsasl2.so.3.0.0, libsbc.so.1.2.1, libseccomp.so.2.5.2, libsecret-1.so.0.0.0, libselinux.so.1, libsemanage.so.1, libsepol.so.1, libshout.so.3.2.0, libsigsegv.so.2.0.4, libslapi-2.4.so.2.10.9, libslirp.so.0.2.3, libsmartcols.so.1.1.0, libsmbclient.so.0.7.0, libsmbconf.so.0.0.1, libsmbios_c.so.2.2.1, libsmbldap.so.2.1.0, libsmime3.so, libSM.so.6.0.1, libsndfile.so.1.0.28, libsoftokn3.so, libsolvext.so.1, libsolv.so.1, libsoup-2.4.so.1.8.0, libsoup-gnome-2.4.so.1.8.0, libspeexdsp.so.1.5.0, libspeex.so.1.5.1, libsqlite3.so.0.8.6, libssh.so.4.8.7, libssl3.so, libssl.so.1.1.1k, libss.so.2.0, libstartup-notification-1.so.0.0.0, libstdc++.so.6.0.25, libsubid.so.3.0.0, libsystemd.so.0.23.0, libtag_c.so.0.0.0, libtag.so.1.17.0, libtalloc.so.2.3.4, libtasn1.so.6.5.5, libtbbmalloc_proxy.so.2, libtbbmalloc.so.2, libtbb.so.2, libtcl8.6.so, libtclenvmodules.so, libtdb.so.1.4.7, libtevent.so.0.13.0, libtevent-util.so.0.0.1, libthai.so.0.3.0,

libtheoradec.so.1.1.4, libtheoraenc.so.1.1.2, libtheora.so.0.3.10, libthread_db-1.0.so, libtic.so.6.1, libtiff.so.5.3.0, libtiffxx.so.5.3.0, libtinfo.so.6.1, libtirpc.so.3.0.0, libtotem-plparser-mini.so.18.1.2, libtotem-plparser.so.18.1.2, libtspi.so.1.2.0, libtss2-esys.so.0.0.0, libtss2-mu.so.0.0.0, libtss2-rc.so.0.0.0, libtss2-sys.so.0.0.0, libtss2-tcti-device.so.0.0.0, libtss2-tctildr.so.0.0.0, libtss2-tcti-mssim.so.0.0.0, libtwolame.so.0.0.0, libudev.so.1.6.11, libudisks2.so.0.0.0, libulockmgr.so.1.0.1, libunbound.so.2.7.18, libunistring.so.2.1.0, libupower-glib.so.3.0.1, libusb-1.0.so.0.2.0, libusbguard.so.1.0.0, libusbmuxd.so.4.0.0, libuser_files.so, libuser_ldap.so, libuser_shadow.so, libuser.so.1.5.2, libutempter.so.1.1.6, libutil-2.28.so, libuuid.so.1.3.0, ov511-decomp, ov518-decomp, v4l1compat.so, v4l2convert.so, libv4l-mplane.so, libv4l1.so.0.0.0, libv4l2rds.so.0.0.0, libv4l2.so.0.0.0, libv4lconvert.so.0.0.0, libverto.so.1.0.0, libvisual-0.4.so.0.0.0, libvolume_key.so.1.2.3, libvorbisenc.so.2.0.11, libvorbisfile.so.3.3.7, libvorbis.so.0.4.8, libvpx.so.5.0.0, libvte-2.91.so.0.5200.4, libwacom.so.2.6.1, libwavpack.so.1.2.0, libwayland-client.so.0.21.0, libwayland-cursor.so.0.21.0, libwayland-egl.so.1.21.0, libwayland-server.so.0.21.0, libwebkit2gtk-4.0.so.37.57.8, libwebpdecoder.so.3.0.2, libwebpdemux.so.2.0.4, libwebpmux.so.3.0.2, libwebp.so.7.0.2, libwebrtc_audio_processing.so.1.0.0, libwoff2common.so.1.0.2, libwoff2dec.so.1.0.2, libwoff2enc.so.1.0.2, libwpe-1.0.so.1.5.1, libWPEBackend-fdo-1.0.so.1.8.3, libX11.so.6.3.0, libX11-xcb.so.1.0.0, libXau.so.6.0.0, libxcb-composite.so.0.0.0, libxcb-damage.so.0.0.0, libxcb-dpms.so.0.0.0, libxcb-dri2.so.0.0.0, libxcb-dri3.so.0.0.0, libxcb-ewmh.so.2.0.0, libxcb-glx.so.0.0.0, libxcb-icccm.so.4.0.0, libxcb-image.so.0.0.0, libxcb-keysyms.so.1.0.0, libxcb-present.so.0.0.0, libxcb-randr.so.0.1.0, libxcb-record.so.0.0.0, libxcb-render.so.0.0.0, libxcb-render-util.so.0.0.0, libxcb-res.so.0.0.0, libxcb-screensaver.so.0.0.0, libxcb-shape.so.0.0.0, libxcb-shm.so.0.0.0, libxcb.so.1.1.0, libxcb-sync.so.1.0.0, libxcb-util.so.1.0.0, libxcb-xf86dri.so.0.0.0, libxcb-xfixes.so.0.0.0, libxcb-xinerama.so.0.0.0, libxcb-xinput.so.0.1.0, libxcb-xkb.so.1.0.0, libxcb-xselinux.so.0.0.0, libxcb-xtest.so.0.0.0, libxcb-xvmc.so.0.0.0, libxcb-xv.so.0.0.0, libXcomposite.so.1.0.0, libXcursor.so.1.0.2, libXdamage.so.1.1.0, libXdmcp.so.6.0.0, libXext.so.6.4.0, libXfixes.so.3.1.0, libXfont2.so.2.0.0, libXft.so.2.3.3, libXinerama.so.1.0.0, libXi.so.6.1.0, libxkbcommon.so.0.0.0, libxkbcommon-x11.so.0.0.0, libxkbfile.so.1.0.2, libxklavier.so.16.4.0, libxml2.so.2.9.7, libxmlb.so.1.0.0, libxmlsec1-openssl.so.1.2.25, libxmlsec1.so.1.2.25, libXmu.so.6.2.0, libXmuu.so.1.0.0, libXrandr.so.2.2.0, libXrender.so.1.3.0, libxshmfence.so.1.0.0, libxslt.so.1.1.32, libxtables.so.12.2.0, libXt.so.6.0.0, libXtst.so.6.1.0, libXvMC.so.1.0.0, libXvMCW.so.1.0.0, libXv.so.1.0.0, libXxf86misc.so.1.1.0, libXxf86vm.so.1.0.0, libyaml-0.so.2.0.5, libz.so.1.2.11, libzstd.so.1.4.4, LLVMgold.so, lpeg.so.1.0.1, lxp.so, core.so, serial.so, unix.so, libman-2.7.6.1.so, libmandb-2.7.6.1.so, libmm-plugin-altair-lte.so, libmm-plugin-anydata.so, libmm-plugin-broadmobi.so, libmm-plugin-cinterion.so, libmm-plugin-dell.so, libmm-plugin-dlink.so, libmm-plugin-ericsson-mbm.so, libmm-plugin-fibocom.so, libmm-plugin-foxconn.so, libmm-plugin-generic.so, libmm-plugin-gosuncn.so, libmm-plugin-haier.so, libmm-plugin-huawei.so, libmm-plugin-intel.so, libmm-plugin-iridium.so, libmm-plugin-linktop.so, libmm-plugin-longcheer.so, libmm-plugin-motorola.so, libmm-plugin-mtk.so, libmm-plugin-nokia-icera.so, libmm-plugin-nokia.so, libmm-plugin-novatel-lte.so, libmm-plugin-novatel.so, libmm-plugin-option-hso.so, libmm-plugin-option.so, libmm-plugin-pantech.so, libmm-plugin-qcom-soc.so, libmm-plugin-quectel.so, libmm-plugin-samsung.so, libmm-plugin-sierra-legacy.so, libmm-plugin-sierra.so, libmm-plugin-simtech.so, libmm-plugin-telit.so, libmm-plugin-thuraya.so, libmm-plugin-tplink.so, libmm-plugin-ublox.so, libmm-plugin-via.so, libmm-plugin-wavecom.so, libmm-plugin-x22x.so, libmm-plugin-zte.so, libmm-shared-fibocom.so, libmm-shared-foxconn.so, libmm-shared-icera.so, libmm-shared-novatel.so, libmm-shared-option.so, libmm-shared-sierra.so, libmm-shared-telit.so, libmm-shared-xmm.so, libmutter-clutter-4.so.0.0.0, libmutter-cogl-4.so.0.0.0, libmutter-cogl-gles2-4.so.0.0.0, libmutter-cogl-pango-4.so.0.0.0, libmutter-cogl-path-4.so.0.0.0, libdefault.so, libnm-vpn-plugin-libreswan-editor.so, libnm-vpn-plugin-libreswan.so, libnm-device-plugin-wifi.so, libnm-device-plugin-wwan.so, libnm-settings-plugin-ifcfg-rh.so, libnm-wwan.so, bltest, dbtool, derdump, ecperf,

fbectest, fipstest, listsuites, ocspclnt, pp, selfserv, shlibsign, signtool, strsclnt, symkeyutil, tstclnt, validation, vfychain, vfyserv, B.so, Fcntl.so, DosGlob.so, Glob.so, GDBM_File.so, Util.so, FieldHash.so, Langinfo.so, IO.so, NDBM_File.so, ODBM_File.so, Opcode.so, POSIX.so, encoding.so, mmap.so, scalar.so, via.so, SDBM_File.so, Hostname.so, NamedCapture.so, arybase.so, attributes.so, mro.so, re.so, Cwd.so, Encode.so, Byte.so, CN.so, EBCDIC.so, JP.so, KR.so, Symbol.so, TW.so, Unicode.so, Base64.so, Socket.so, Storable.so, Normalize.so, threads.so, shared.so, libpipewire-module-access.so, libpipewire-module-adapter.so, libpipewire-module-client-device.so, libpipewire-module-client-node.so, libpipewire-module-link-factory.so, libpipewire-module-metadata.so, libpipewire-module-portal.so, libpipewire-module-profiler.so, libpipewire-module-protocol-native.so, libpipewire-module-rtkit.so, libpipewire-module-session-manager.so, libpipewire-module-spa-device-factory.so, libpipewire-module-spa-device.so, libpipewire-module-spa-node-factory.so, libpipewire-module-spa-node.so, gnome-keyring-pkcs11.so, p11-kit-trust.so, details.so, label.so, text.so, tribar.so, two-step.so, drm.so, frame-buffer.so, libalsa-util.so, libbluez5-util.so, libcli.so, libprotocol-cli.so, libprotocol-esound.so, libprotocol-http.so, libprotocol-native.so, libprotocol-simple.so, librtp.so, libwebrtc-util.so, module-allow-passthrough.so, module-alsa-card.so, module-alsa-sink.so, module-alsa-source.so, module-always-sink.so, module-always-source.so, module-augment-properties.so, module-bluetooth-discover.so, module-bluetooth-policy.so, module-bluez5-device.so, module-bluez5-discover.so, module-card-restore.so, module-cli-protocol-tcp.so, module-cli-protocol-unix.so, module-cli.so, module-combine-sink.so, module-combine.so, module-console-kit.so, module-dbus-protocol.so, module-default-device-restore.so, module-device-manager.so, module-device-restore.so, module-echo-cancel.so, module-esound-compat-spawnfd.so, module-esound-compat-spawnpid.so, module-esound-protocol-tcp.so, module-esound-protocol-unix.so, module-esound-sink.so, module-filter-apply.so, module-filter-heuristics.so, module-hal-detect.so, module-http-protocol-tcp.so, module-http-protocol-unix.so, module-intended-roles.so, module-ladspa-sink.so, module-loopback.so, module-match.so, module-mmkbd-evdev.so, module-native-protocol-fd.so, module-native-protocol-tcp.so, module-native-protocol-unix.so, module-null-sink.so, module-null-source.so, module-pipe-sink.so, module-pipe-source.so, module-position-event-sounds.so, module-remap-sink.so, module-remap-source.so, module-rescue-streams.so, module-role-cork.so, module-role-ducking.so, module-rtp-recv.so, module-rtp-send.so, module-rygel-media-server.so, module-simple-protocol-tcp.so, module-simple-protocol-unix.so, module-sine-source.so, module-sine.so, module-stream-restore.so, module-suspend-on-idle.so, module-switch-on-connect.so, module-switch-on-port-available.so, module-systemd-login.so, module-tunnel-sink-new.so, module-tunnel-sink.so, module-tunnel-source-new.so, module-tunnel-source.so, module-udev-detect.so, module-virtual-sink.so, module-virtual-source.so, module-virtual-surround-sink.so, module-volume-restore.so, libpulsecommon-14.0.so, libpulsecore-14.0.so, libpulsedsp.so, _audit.so, _dbus_bindings.so, _dbus_glib_bindings.so, _selinux.cpython-36m-x86_64-linux-gnu.so, _semanage.cpython-36m-x86_64-linux-gnu.so, _yaml.cpython-36m-x86_64-linux-gnu.so, auparse.so, dmidecodemod.cpython-36m-x86_64-linux-gnu.so, ethtool.cpython-36m-x86_64-linux-gnu.so, libxml2mod.so, _cairo.cpython-36m-x86_64-linux-gnu.so, _gi.cpython-36m-x86_64-linux-gnu.so, _gi_cairo.cpython-36m-x86_64-linux-gnu.so, _gpgme.cpython-36m-x86_64-linux-gnu.so, _hawkey.so, _hawkey_test.so, _libpycomps.so, _common_types.so, _conf.so, _error.so, _module.so, _repo.so, _smartcols.so, _transaction.so, _utils.so, _librepo.so, _certificate.cpython-36m-x86_64-linux-gnu.so, _rpm.cpython-36m-x86_64-linux-gnu.so, _rpm.so, _rpmb.cpython-36m-x86_64-linux-gnu.so, _rpmb.so, _rpms.cpython-36m-x86_64-linux-gnu.so, _rpms.so, audit2why.cpython-36m-x86_64-linux-gnu.so, policyrep.cpython-36m-x86_64-linux-gnu.so, _daemon.cpython-36m-x86_64-linux-gnu.so, _journal.cpython-36m-x86_64-linux-gnu.so, _reader.cpython-36m-x86_64-linux-gnu.so, id128.cpython-36m-x86_64-linux-gnu.so, login.cpython-36m-x86_64-linux-gnu.so, libqconnmanbearer.so, libqgenericbearer.so, libqnmbearer.so, libqeglfs-emu-integration.so, libqeglfs-kms-egldevice-integration.so, libqeglfs-kms-integration.so, libqeglfs-x11-

integration.so, libqevdevkeyboardplugin.so, libqevdevmouseplugin.so, libqevdevtabletplugin.so, libqevdevtouchplugin.so, libqlibinputplugin.so, libqtuiotouchplugin.so, libqgif.so, libqico.so, libqjpeg.so, libcomposeplatforminputcontextplugin.so, libibusplatforminputcontextplugin.so, libqeglfs.so, libqlinuxfb.so, libqminimal.so, libqminimalegl.so, libqoffscreen.so, libqvnc.so, libqxcb.so, libqgtk3.so, libqxdgdesktopportal.so, libcupsprintersupport.so, libqmldbg_debugger.so, libqmldbg_inspector.so, libqmldbg_local.so, libqmldbg_messages.so, libqmldbg_native.so, libqmldbg_nativedebugger.so, libqmldbg_preview.so, libqmldbg_profiler.so, libqmldbg_quickprofiler.so, libqmldbg_server.so, libqmldbg_tcp.so, libqsqlite.so, libqxcb-egl-integration.so, libqxcb-glx-integration.so, liblabsanimationplugin.so, libqmlfolderlistmodelplugin.so, liblabsmodelsplugin.so, libqmlsettingsplugin.so, libsharedimageplugin.so, libqmlwavefrontmeshplugin.so, libqmlplugin.so, libmodelsplugin.so, libqtqmlstatemachine.so, libworkerscriptplugin.so, libqquicklayoutsplugin.so, libqmllocalstorageplugin.so, libparticlesplugin.so, libqmlshapesplugin.so, libwindowplugin.so, libqmlxmllistmodelplugin.so, libqtquick2plugin.so, libqmltestplugin.so, selinux.so, fmhash.so, fmhttp.so, imdiag.so, imfile.so, imjournal.so, imklog.so, immark.so, impstats.so, imptcp.so, imtcp.so, imudp.so, imuxsock.so, lmnet.so, lmnetstrms.so, lmnsd_gtls.so, lmnsd_ptcp.so, lmregexp.so, lmtcpclt.so, lmtcpsrv.so, lmzlibw.so, mmanon.so, mmcount.so, mmexternal.so, mmutf8fix.so, omhttp.so, omjournal.so, ommail.so, omprog.so, omstdout.so, omtesting.so, omuxsock.so, pmaixforwardedfrom.so, pmcisconames.so, pmlastmsg.so, pmsnare.so, libCHARSET3-samba4.so, libMESSAGING-SEND-samba4.so, libMESSAGING-samba4.so, libaddns-samba4.so, libads-samba4.so, libasn1util-samba4.so, libauth-samba4.so, libauthkrb5-samba4.so, libcli-cldap-samba4.so, libcli-ldap-common-samba4.so, libcli-ldap-samba4.so, libcli-nbt-samba4.so, libcli-smb-common-samba4.so, libcli-spoolss-samba4.so, libcliauth-samba4.so, libclidns-samba4.so, libcluster-samba4.so, libcmdline-contexts-samba4.so, libcmdline-samba4.so, libcommon-auth-samba4.so, libctdb-event-client-samba4.so, libdbwrap-samba4.so, libdcerpc-pkt-auth-samba4.so, libdcerpc-samba-samba4.so, libevents-samba4.so, libflag-mapping-samba4.so, libgenrand-samba4.so, libgensec-samba4.so, libgpext-samba4.so, libgpo-samba4.so, libgse-samba4.so, libhttp-samba4.so, libinterfaces-samba4.so, libiov-buf-samba4.so, libkrb5samba-samba4.so, libldbsamba-samba4.so, liblibcli-lsa3-samba4.so, liblibcli-netlogon3-samba4.so, liblibsmb-samba4.so, libmessages-dgm-samba4.so, libmessages-util-samba4.so, libmscat-samba4.so, libmsghdr-samba4.so, libmsrpc3-samba4.so, libndr-samba-samba4.so, libndr-samba4.so, libnet-keytab-samba4.so, libnetif-samba4.so, libnpa-tstream-samba4.so, libposix-eadb-samba4.so, libprinter-driver-samba4.so, libprinting-migrate-samba4.so, libregistry-samba4.so, libreplace-samba4.so, libsamba-cluster-support-samba4.so, libsamba-debug-samba4.so, libsamba-modules-samba4.so, libsamba-security-samba4.so, libsamba-sockets-samba4.so, libsamba3-util-samba4.so, libsamdb-common-samba4.so, libsecrets3-samba4.so, libserver-id-db-samba4.so, libserver-role-samba4.so, libsmb-transport-samba4.so, libsmbclient-raw-samba4.so, libsmbd-base-samba4.so, libsmbd-shim-samba4.so, libsmbldaphelper-samba4.so, libsocket-blocking-samba4.so, libsys-rw-samba4.so, libtalloc-report-printf-samba4.so, libtalloc-report-samba4.so, libtdb-wrap-samba4.so, libtime-basic-samba4.so, libtorture-samba4.so, libtrusts-util-samba4.so, libutil-reg-samba4.so, libutil-setid-samba4.so, libutil-tdb-samba4.so, ldapsam.so, smbpasswd.so, tdbsam.so, libwbclient.so.0.15, libanonymous.so.3.0.0, libsasldb.so.3.0.0, pam_access.so, pam_cap.so, pam_chroot.so, pam_console.so, pam_cracklib.so, pam_debug.so, pam_deny.so, pam_echo.so, pam_env.so, pam_exec.so, pam_faildelay.so, pam_faillock.so, pam_filter.so, pam_ftp.so, pam_gdm.so, pam_gnome_keyring.so, pam_group.so, pam_issue.so, pam_keyinit.so, pam_lastlog.so, pam_limits.so, pam_listfile.so, pam_localuser.so, pam_loginuid.so, pam_mail.so, pam_mkhomedir.so, pam_motd.so, pam_namespace.so, pam_nologin.so, pam_permit.so, pam_postgresok.so, pam_pwhistory.so, pam_pwquality.so, pam_rhosts.so, pam_rootok.so, pam_securetty.so, pam_selinux.so, pam_sepermit.so, pam_shells.so, pam_stress.so, pam_succeed_if.so, pam_systemd.so, pam_time.so,

pam_timestamp.so, pam_tty_audit.so, pam_umask.so, pam_unix.so, pam_userdb.so, pam_usertype.so, pam_warn.so, pam_wheel.so, pam_xauth.so, libspa-alsa.so, libspa-audioconvert.so, libspa-audiomixer.so, libspa-bluez5.so, libspa-control.so, libspa-dbus.so, libspa-support.so, libspa-v4l2.so, libspa-videoconvert.so, staplog.so, libwebkit2gtkinjectedbundle.so, libexa.so, libfb.so, libfbdevhw.so, libglamoregl.so, libint10.so, libshadow.so, libshadowfb.so, libvbe.so, libvgahw.so, libwfb.so, fbdev_drv.so, intel_drv.so, modesetting_drv.so, vesa_drv.so, libglx.so, libinput_drv.so, libarpt_mangle.so, libebt_802_3.so, libebt_among.so, libebt_arp.so, libebt_arpreply.so, libebt_dnat.so, libebt_ip.so, libebt_ip6.so, libebt_log.so, libebt_mark.so, libebt_mark_m.so, libebt_nflog.so, libebt_pkttype.so, libebt_redirect.so, libebt_snat.so, libebt_stp.so, libebt_vlan.so, libip6t_DNAT.so, libip6t_DNPT.so, libip6t_HL.so, libip6t_LOG.so, libip6t_MASQUERADE.so, libip6t_NETMAP.so, libip6t_REDIRECT.so, libip6t_REJECT.so, libip6t_SNAT.so, libip6t_SNPT.so, libip6t_ah.so, libip6t_dst.so, libip6t_eui64.so, libip6t_frag.so, libip6t_hbh.so, libip6t_hl.so, libip6t_icmp6.so, libip6t_ipv6header.so, libip6t_mh.so, libip6t_rt.so, libip6t_srh.so, libipt_CLUSTERIP.so, libipt_DNAT.so, libipt_ECN.so, libipt_LOG.so, libipt_MASQUERADE.so, libipt_NETMAP.so, libipt_REDIRECT.so, libipt_REJECT.so, libipt_SNAT.so, libipt_TTL.so, libipt_ULOG.so, libipt_ah.so, libipt_icmp.so, libipt_realm.so, libipt_ttl.so, libxt_AUDIT.so, libxt_CHECKSUM.so, libxt_CLASSIFY.so, libxt_CONNMARK.so, libxt_CONNSECMARK.so, libxt_CT.so, libxt_DSCP.so, libxt_HMARK.so, libxt_IDLETIMER.so, libxt_LED.so, libxt_MARK.so, libxt_NFLOG.so, libxt_NFQUEUE.so, libxt_RATEEST.so, libxt_SECMARK.so, libxt_SET.so, libxt_SYNPROXY.so, libxt_TCPMSS.so, libxt_TCPOPTSTRIP.so, libxt_TEE.so, libxt_TOS.so, libxt_TPROXY.so, libxt_TRACE.so, libxt_addrtype.so, libxt_bpf.so, libxt_cgroup.so, libxt_cluster.so, libxt_comment.so, libxt_connbytes.so, libxt_connlabel.so, libxt_connlimit.so, libxt_connmark.so, libxt_conntrack.so, libxt_cpu.so, libxt_dccp.so, libxt_devgroup.so, libxt_dscp.so, libxt_ecn.so, libxt_esp.so, libxt_hashlimit.so, libxt_helper.so, libxt_ipcomp.so, libxt_iprange.so, libxt_ipvs.so, libxt_length.so, libxt_limit.so, libxt_mac.so, libxt_mark.so, libxt_multiport.so, libxt_nfacct.so, libxt_osf.so, libxt_owner.so, libxt_physdev.so, libxt_pkttype.so, libxt_policy.so, libxt_quota.so, libxt_rateest.so, libxt_recent.so, libxt_rpfilter.so, libxt_sctp.so, libxt_set.so, libxt_socket.so, libxt_standard.so, libxt_statistic.so, libxt_string.so, libxt_tcp.so, libxt_tcpmss.so, libxt_time.so, libxt_tos.so, libxt_u32.so, libxt_udp.so