Rosie Device-Level Threat And Vulnerability Assessment

v6 2022-08-25

Stephen Warren

Roopa Prabhu

Table of Contents

Table of Contents 2

Revision History 3

Introduction 4

References 4

Definitions 4

Identification of Target of Evaluation 5

Environmental Assumptions 6

Security Assets 6

Attacker Models and Motivations 7

    Examples of Attacks/Attackers 8

Threat Model Diagram 11

Security Objectives 11

Revision History

Author	Date	Changes
swarren	v1 2020-07-01	Initial Draft.
swarren	v2 2020-07-02	Minor clarifications in text.
swarren	v3 2020-07-07	Link to cloud backend TAVA. Fixed a couple minor typos.
swarren	v4 2020-07-08	● Enhanced OBJ-1 to address level of access. ● Added definitions of “access” and “data” to the objectives section. ● Added OBJ-19; defense in depth.
swarren	v5 2020-07-21	● Added OBJ-20; legitimate users can only access the device as intended. ● ReLingo: Replace “black box”. ● Fix typo in DDos definition.
roopa	V6 2022-08-25	- Added threat model created in msft tool - Added stride classification to threats - Added security requirements - Other new design cleanups

Introduction

This document contains a Threat and Vulnerability Analysis for the Rosie device.

References

- EGX Confluence
- EGX Cloud Services - TAVA (A rough model for this document. Broad document structure and some specific text was lifted from this document.)
- Rosie - Product Definition
- Rosie Cloud Backend TAVA WIP
- <mobile app TAVA or SADD>

Definitions

Term	Definition
AI	Artificial Intelligence. The application of computing power to the analysis of data.
DNS	Domain Name System. A network service that translates textual host or domain names into numerical IP addresses, and related directory information.
DDoS	Distributed Denial of Service. A network-based attack where a large set of systems is commanded to send a high bandwidth stream of network packets to a designated target. This typically prevents the target from performing its intended task.
DoS	Denial of Service. The prevention of a system from performing its designated task or providing a service.
EGX	NVIDIA's cloud-based compute/AI endpoint management system.
Gem	A Rosie/DeepStream software component which analyzes a video stream to extract some form of metadata. These may be bundled with the base Rosie software image, or potentially installed onto a Rosie system by an end-user or system integrator during or after deployment.
HDMI	High-Definition Multimedia Interface. A standard interface to transfer graphical images from a computer system to a display device.

IT	Information Technology. Commonly used within the phrase “IT department”, which indicates the portion of a business dedicated to managing computer, network, and/or telephony systems.
MITM	Man in the Middle. A network attack where an imposter system interposes itself in the middle of a communication channel and impersonates the server to the client, and the client to the server. A successful attack typically allows the imposter to eavesdrop and/or modify arbitrary data within the communication channel.
NVR	Network Video Recorder. A device which records video streams to local storage, and allows live or subsequent viewing of that video data via a network connection.
ODM	Original Design Manufacturer. In this context, designs and manufactures hardware systems.
OEM	Original Equipment Manufacturer. In this context, contracts with an ODM to design and manufacture a hardware system, then applies their own branding to the system prior to retail or B2B (business-to-business) sales.
OS	Operating System. Software that provides the interface between application software and hardware, including e.g. task switching, resource sharing, device drivers, network communication, etc.
SMS	Short Messaging Service. An alternate name for texting or text messaging, as implemented by a telephone network.
TAVA	Threat and Vulnerability Analysis.
USB	Universal Serial Bus. A standard interface between a computer system and a peripheral. In this context, most relevant for keyboards and mice.

Identification of Target of Evaluation

Rosie is an intelligent NVR. It is a physical device which connects to security cameras, captures video streams from the cameras to local disk, analyzes the video data to produce metadata such as people counts or proximity alerts, allows viewing of live and historical recordings and analysis, and provides alerts to its users. Rosie is deployed on-site along with video cameras. These sites do not generally have an IT department. Rosie is managed and used by end-users, likely as a secondary aspect of their job. Rosie may be accessed by legitimate users either over the local network, or from any location with Internet access.

This TAVA concentrates on the Rosie device (as a whole; without internal decomposition), and its interface to users or other systems. Rosie relies on cloud-based backend service, e.g. to assist in mobile client auth, remote access and alerting. For the purposes of this TAVA, these

are considered as opaque services; the cloud services themselves will be analyzed in a separate TAVA.

Environmental Assumptions

Rosie is an EGX node, and Rosie application software is packaged as containers that are launched by EGX.

EGX is expected to provide certain system/OS-level protections, such as integrating with system-level secure boot, protecting its own connection to the EGX cloud backend, etc. However, since this TAVA addresses Rosie as an undecomposed system, requirements that apply to or are satisfied by EGX are not called out separately nor omitted.

EGX itself does not provide Rosie with Rosie-specific features. EGX is responsible for e.g. update of the EGX OS, update and launch of the Rosie container, etc. However, EGX does not provide any Rosie-specific functionality such as dynamic DNS service, application-specific proxy servers, end-user-facing user-interface or applications, etc.

Rosie devices are manufactured by ODMs, not by NVIDIA.

Rosie devices are branded by OEMs, not by NVIDIA.

Rosie is connected to a potentially hostile network. For example, Rosie's owner may choose to attach Rosie to the same network that provides the owner's customers with WiFi access. Rosie will not be accessed by network-based client applications. Rosie device will only be connected to Rosie cloud backend. Rosie mobile client access will be relayed to in the form of API calls via the trusted rosie cloud backend. No Rosie mobile client will have direct access to Rosie devices.

Rosie device has pre configured default Linux firewall rules which disables all incoming traffic, all outgoing traffic except for ports DNS, TCP Mux, HTTPS, HTTP. All outgoing UDP ports are kept open for WebRTC traffic.

Rosie is deployed to sites that may not have complete physical access control. Some sites may install Rosie in a locked back room. Other sites may install Rosie in a location accessible from the store front, such as alongside/nearby a cash register.

Rosie supports direct connection of USB input devices and HDMI/similar display. These will likely support at least status display, if not a full blown application equivalent to a network-based client application. This will be true only for beta release.

Security Assets

Rosie captures, stores, processes, generates, transmits a wide variety of information. Rosie runs valuable software algorithms. Access to or use of the Rosie hardware capabilities may be considered an asset.

- Configuration of the system, such as:
    - Connected device config eg rtsp urls, rtsp username
    - Network configuration.
    - The set of cameras attached to the system.
    - Storage configuration (policies)
    - Security config - policies, encryption, etc
    - kiosk with camera, microphone and speaker connected to the system.
    - The type of analysis to perform on each video and audio stream, and any parameters for that analysis (regions of interest, calendars, etc.).
    - Root and client certificates
    - MAC (Mandatory Access Control) policies
    - Kernel configuration (Kernel boot parameters, persistent and non-persistent kernel configuration, cryptographic keys in kernel keyring)
- Identity and authentication credentials:
    - For users of the system (authentication).
    - For access to cameras (authentication).
    - For access to cloud-based backend services (authentication).
    - For provision of services to client applications (identity).
- Device identities for device authentication
- Live video streams.
- Historical video streams.
- Live metadata/analysis extracted from video streams.
- Metadata/analysis previously extracted from video streams.
- Personal information of users of the system, mainly for sending alerts, or as recovery options for login credentials, such as:
    - Email addresses.
    - Phone numbers (for SMS/text).
- Software (e.g. EGX OS, EGX application, Rosie application).
- Software algorithms (e.g. AI video analysis implementations).
- Audit logs.
- Disk storage space.
- CPU/GPU processor time.
- Network access/bandwidth.
- Device.

Assets not expected to be present in the first public release of Rosie include:

- End-user financial information.

These may appear later as support for user-installed for-pay Gems is added to the system.

Assets not in scope of this TAVA:

- EGX stack TAVA
- Rosie mobile client TAVA
- TAVA for individual microservices used by Rosie (eg Deepstream, Riva and other microservices have their own TAVA documents)

Attacker Models and Motivations

Attacker capabilities for the purpose of the TAVA for Rosie are assumed to have high capability. In common criteria terms, the attackers are potentially expert level at their most capable. The development of this attacker model derives from the fact that Rosie is at least partially exposed to the Internet at large and implements security-related functionality. Thus, Rosie may attract arbitrary attackers even if only accidentally. However, since Rosie is aimed at small installations, multiple expert level attackers are expected not to concentrate on Rosie, since their sights may be set on higher value systems.

Attacks on Rosie may fall into two broad categories:

- Generic attacks on an arbitrary device. Such attacks apply to any computing device, with common/well-known objectives such as password theft, CPU time theft, DDoS launch, or general DoS.
- Rosie-specific attacks, such as video reconnaissance, or disabling site security/monitoring prior to launching a physical attack.

In both of the above categories, threats can be further categorized into local, remote and physical attacks. Insider attacks, by past end-users or employees of HW or SW vendors, are considered in-scope.

Discussion of attacker motivations is not meant to be an exhaustive list of all possible attacker motivations for executing attacks upon Rosie. However, it is meant to convey the general behavior, capabilities, and motivations of the attackers to ensure that the proper security objectives, requirements, and vulnerability analysis is completed. A pessimistic approach is taken to ensure that adequate defense-in-depth is put in place.

Examples of Attacks/Attackers

Attacks are marked with Spoofing Identity (S), Tampering with data (T), Repudiation threats (R), Information disclosure (I), Denial of service (D) and Elevation of privileges (E) following the STRIDE method.

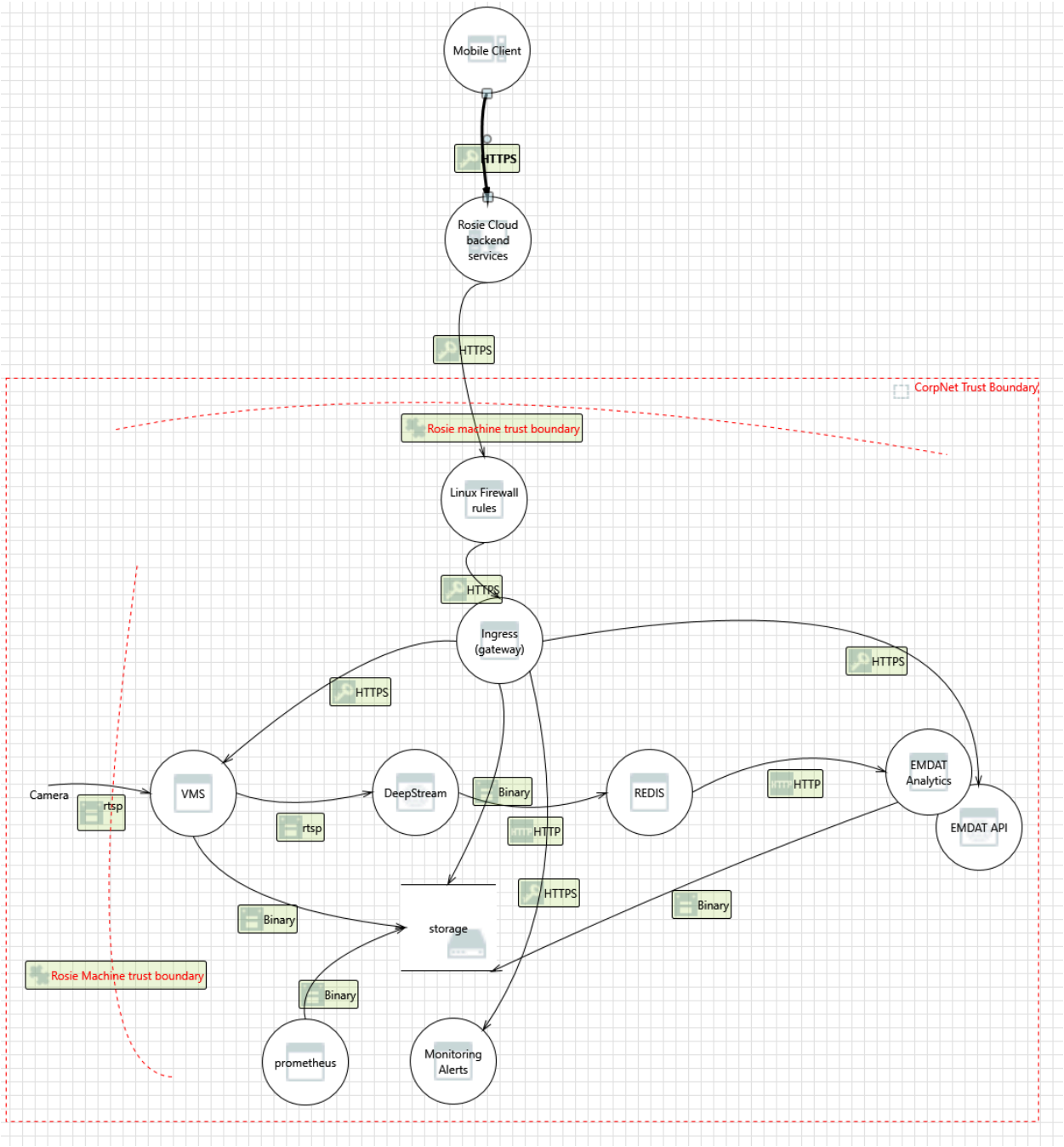
- Plain destruction of data (T,D):
    - Attacker destroys system configuration or stored data.
    - Motivated by a quest for power or lust for destruction.
- Execution of any malicious payload (D, E):
    - Attacker temporarily denies access to the system or specific data or runs with elevated privileges.
    - Motivated by financial gain when the system owner pays to terminate the DoS.
- Theft of CPU/GPU resources (D):
    - Attacker runs e.g. a Bitcoin miner on Rosie.
    - Motivated by financial gain via sale of bitcoin.
- Use of network bandwidth (D):
    - Attackers run software to send a high volume of outbound network traffic.
    - Motivated by a quest for power, or by financial gain via payment to start or stop a DDos against an unrelated target.
- Theft of end-user password (S, I):
    - Attacker obtains and cracks the password file, then attempts to sell or re-use those credentials on other services.
    - Motivated by financial gain via sale of credentials, or access to other valuable services in the end-user's name.
- Theft of system credentials (S,I):
    - Attackers steal the system's credentials, which allows them to masquerade as the system to other services.
    - For example, may allow access to send spam emails using the system's cloud credentials.
    - For example, may allow a camera to be replaced, which provides a fake video stream, which prevents recording of a crime.
- Theft of contact/location information (I):
    - Attackers extracts valid email addresses or phone numbers from the system, then sells them to spammers or sends spam themself.
    - Motivated by financial gain via sale of contact information or generation of funds via spamming.
- Theft of video data and/or analytics (I):
    - Motivated by competitive knowledge of the owner's business health.
    - Motivated by tracking an individual who entered the owner's store.
- Theft of software (I,S):
    - Attacker steals software from Rosie and analyzes or uses it.
    - Rosie-based software implements advanced video analysis.

    - Motivated by a desire to reverse engineer the algorithm for a competitive product.
    - Motivated by a desire to use the software without paying for a genuine Rosie system.
- Theft of device storage (I):
    - Attacker steals Rosie, removes the storage device, and extracts data from it using another computer system.
    - Motivated by access to private information.
- Theft of device (I):
    - Attacker steals Rosie, and attempts to interact with it via console or network.
    - Motivated by access to private information.
- Illegitimate physical access (I, D, T, E):
    - Attacker connects some device to a physical port on Rosie and attempts to interact with Rosie via that port.
    - Attacker launches DMA attacks.
    - Motivated by access to private information, or DoS.
- Targeted modification of system configuration and software (S,T,I,R):
    - Attacker modifies some arbitrary configuration of the Rosie software.
    - Attacker tricks the system into running an older insecure version of software (eg software rollback attacks)
    - Motivated by a desire to hide some upcoming video-based event that the system would otherwise capture and alert on.
    - Motivated by a desire to hide some upcoming log or audit event.
    - Motivated by a desire to cause problems for the system owner (e.g. disgruntled employee).
- Targeted destruction of data (T):
    - Attacker removes/destroys some recorded data.
    - Motivated by a desire to remove video evidence of a past event.
    - Motivated by a desire to remove log or audit messages related to some previous system access or configuration change.
- Installation of persistent software and firmware (D,E):
    - Attacker installs software that runs on the system even after the attacker has disconnected.
    - Motivated by a desire to spy on the physical location via cameras.
    - Motivated by a desire to extract data from the system at an arbitrary time in the future.
    - Motivated by a desire to collect access to systems for the later execution of a DDos attack, spamming, or other action.
- Network Interposition - Cloud Backend (S, I, T, D)
    - Attacker inserts a network device into the path between Rosie and its cloud backend services. The inserted device may capture credentials, eavesdrop on or manipulate command/control or video streams.
    - Motivated by credential theft, and potential re-use on other sites.
    - Motivated by a desire to breach privacy.

    - Motivated by a desire to control/reconfigure the cloud backend service via a potentially privileged/feature-rich command path from Rosie.
    - Motivated by a desire to control Rosie via a potentially privileged command path from the cloud.

Many more possibilities exist!

Threat Model Diagram



Raw threat model diagram is [here]

Security Objectives

Derived from the description of Rosie, the asset list, and the attacker model, the security objectives for Rosie are listed below. The functional security requirements are categorized using CIAAA attributes.

Within this list of objectives, the following terms are used:

- Access: Any form of read, write, edit, or delete control over data.
- Data: Any form of data, including the following on-limiting list: video streams, extracted metadata, OS or application code, system configuration, authentication credentials, log files, etc.

ID	Attribute	Description
OBJ-1	Confidentiality, Integrity	Only legitimate users shall be permitted access to, or direct/indirect use of, Rosie or the data it contains in any way, and any access that is granted must be consistent with that user's defined access level. *(e.g. all local application usage or network connections or requests are authenticated.)*
OBJ-2	Confidentiality	It shall not be possible to directly extract any data or information from the storage device of a Rosie system. *(i.e. storage mediums shall be encrypted in such a manner that only the specific legitimate Rosie system can access it.)*
OBJ-3	Confidentiality Integrity	Data transmitted to, from or within a Rosie system shall not be exposed to eavesdropping or tampering. *(i.e. all communications are encrypted and signed.)*
OBJ-4	Integrity	A Rosie system shall only execute authorized software. *(e.g. that shipped by the OEM, or that which the end-user installs from an OEM-sanctioned "app store", or updates.)*
OBJ-5	Integrity	A Rosie system shall not be able to act as a launching point for attack on any other device *(e.g. participation in DDoS, local network reconnaissance, etc.)*
OBJ-6	Availability Authenticity	The behaviour of any network element, besides legitimate Rosie cloud services or users, shall not affect the behaviour or

		availability of Rosie itself, at least in terms of Rosie's own operation. *(Clearly an external network outage is not something Rosie itself controls.)*
OBJ-7	Availability Authenticity	The behaviour of any device or user attached to a physical port on Rosie, besides authenticated users, shall not affect the behaviour or availability of Rosie itself, at least in terms of Rosie's own operation. *(Physically destructive acts such as connecting mains power to a Rosie USB port are out of scope)*
OBJ-8	Authenticity, Integrity	Rosie shall only communicate with and trust legitimate cloud services *(e.g. TLS certificates of those cloud services must be validated)*
OBJ-9	Authenticity, Integrity	Rosie shall only communicate with legitimate cameras. *(e.g. TLS certificates of those cameras must be validated)*
OBJ-10	Integrity, Accountability	Rosie must maintain an accurate view of time. *(e.g. for associating with video or derived metadata, or for log timestamps.)*
OBJ-11	Accountability	Rosie must maintain a log of all authentication events, which may be reviewed by authorized users. *(e.g. user addition or removal, password change, login, logout.)*
OBJ-12	Accountability	Rosie must maintain a log of all configuration events, which may be reviewed by authorized users. *(e.g. adding/removing cameras, enabling/disabling video processing features, modification of tripwires, etc.)*
OBJ-13	Accountability	Rosie must maintain a log of all gaps in service, which may be reviewed by authorized users. *(e.g. camera offline/online, power cycles or reboots of Rosie, process crashes, system anomalies,* OS access control violations, *cloud connection outage, inability to send alerts.)*
OBJ-14	Availability, Integrity	Rosie must monitor its own hardware, to the extent possible, for any issues that do or may affect its correct operation.

		(e.g. SMART monitoring for storage, chip or system temperature monitoring.)
OBJ-15	Integrity	Rosie shall not contain any hard-coded/default-enabled debug/backdoor login, debug logging, any software meant for debug and development purposes or other similar mechanism in a shipping configuration. Such features may exist if not enabled by default, and if they require a legitimate user to enable them. *(Don't leave side channels.)*
OBJ-16	Integrity, Authenticity	Rosie shall use either NIST- or IETF- compliant cryptographic authentication mechanisms. *(Don't roll your own crypto.)*
OBJ-17	Confidentiality, Availability	Rosie must support re-assignment to an unrelated new owner, without exposing the data of one owner to the other, even in the face of physical or network access. *(e.g. a data-hiding factory reset mechanism exists. Any exposed encryption keys are not reused across ownership.)*
OBJ-18	Confidentiality	When a user's access is revoked, this must effectively terminate all access to the system, even if the user is able to later extract more data from the system's storage device or its network communication channels. *(e.g. don't use static or re-used encryption keys for multiple network connections, don't share keys between network and disk encryption.)*
OBJ-19	Confidentiality, Integrity	The system will apply defense-in-depth measures. *In particular, the fact that OBJ-1 disallows access by unauthorized users, or that OBJ-4 disallows unauthorized software from being run, should not be an excuse for software to fail to take individual steps to protect its assets, since bugs happen, and sometimes security objectives are not met despite our best attempts. As such, implementing additional layers of protection is appropriate and encouraged. Examples might be:* ● *Application-/service-level data encryption even when full disk encryption is implemented* ● *Use of an HSM for key storage,*
OBJ-20	Confidentiality,	Legitimate users shall not be able to access the device in any

	Integrity	way not deliberately exposed to/by the “application”. *(e.g. legitimate access to the application should not imply that the user can view, extract, or modify software or internal configuration or data storage of the device.)*
OBJ-21	Confidentiality	Rosie shall not leak any sensitive information

Security Requirements

Administrative Access and User Credentials

Req ID	Obj ID	Priority	Requirement Description
R-AAC-1	OBJ-1, OBJ-8	P0	Rosie system will only communicate with the cloud
R-AAC-2	OBJ-3	P0	All communication to, from and between Rosie components shall be authenticated, encrypted and integrity protected (eg: between cloud and rosie)
R-AAC-3	OBJ-21	P0	Log or config data for Rosie services shall not contain any hard-coded credentials
R-AAC-4	OBJ-11	P0	Audit support for admin and user access (for traceability, accountability, auditability)
R-AAC-5	OBJ-3	P1	Authenticate, encrypt and integrity protect all communications between Rosie microservices
R-ACC-6	OBJ-1	P1	Implement Authentication and authorization for all database accesses

Zero Trust, Network Isolation and Instance Hardening

Req ID	Obj ID	Priority	Requirement Description
R-ZT-1	OBJ-2, OBJ-5	P0	No Rosie microservices and on-prem systems shall be directly exposed to the public Internet
R-ZT-2	OBJ-2, OBJ-5	P0	No Rosie microservices shall be reachable on the local network
R-ZT-3	OBJ-2,OBJ-5	P0	Rosie system will disallow all incoming and outgoing traffic by default and only allow traffic on ports that are serving external users like the Rosie cloud backend
R-ZT-4	OBJ-3	P0	All network/communication traffic between Rosie microservices must be encrypted using TLS1.2 or TLS 1.3 and limited to cipher suites recommended by NVIDIA Product security
R-ZT-5	OBJ-19, OBJ-5	P0	All microservices will run with least-privilege unless absolutely required by the function they provide. No service shall have the privileges to change its own configuration
R-ZT-6	OBJ-4	P0	All software running on Rosie will be from a trusted source (eg NGC for NVidia authored software)
R-ZT-7	OBJ-8, OBJ-5	P0	All API and end points exposed to the network must be tested for malicious input
R-ZT-8	OBJ-2	P0	All data stored on the storage system must be encrypted and integrity protected
R-ZT-9	OBJ-14	P0	Rosie must have smart hardware monitoring and alerting on hardware malfunction by default
R-ZT-10	OBJ-15	P0	Rosie system must disable all forms of login access by default eg ssh must be disabled by default unless the system administrator chooses to enable it. And ssh hardening guidelines must be followed as listed here
R-ZT-11	OBJ-16	P0	Rosie shall use Nvidia certified/recommended/compliant cryptographic authentication mechanisms
R-ZT-12	OBJ-7, OBJ-15	P0	Rosie system should only enable required physical peripheral access. All other unused peripheral device accesses should be disabled by default

R-ZT-13	OBJ-10	P0	All devices in the Rosie system must be synchronized using the same time source
R-ZT-14	OBJ-2	P0	All integrations with third-party or open databases will follow security best practices recommended by the database service
R-ZT-15	OBJ-4, OBJ-5	P0	Rossie microservices are also expected to follow the best security practices such as minimal container images, isolation of microservices, scanning images against known vulnerabilities, orchestration security,
R-ZT-16	OBJ-4, OBJ-5	P0	Rossie software shall be security hardened against memory unsafety issues (stack smashing, user after free, double free, out of bounds access)

Logging, Monitoring, Alerting and Audit

Req ID	Obj ID	Priority	Requirement Description
R-LOG-1	OBJ-11, OBJ-12, OBJ-13	P0	Rosie must log all events, gaps in service for traceability and accountability
R-LOG-2	OBJ-21,	P0	Log, monitoring and audit data stored locally or transmitted remotely shall not contain personally identifiable information unless approved explicitly with proper consent
R-LOG-3	OBJ-11, OBJ-12, OBJ-13	P0	All logging, monitoring and auditing shall contain enough attributes to trace the requesting identity (without sensitive data)

Tenant Isolation and Privacy

Req ID	Obj ID	Priority	Requirement Description
R-TIP-1	OBJ-17, OBJ-18	P0	A Rosie system serving multiple tenants, must have proper isolation and access control per tenant (eg Per tenant data, metadata, storage etc must be properly isolated)

R-TIP-2	OBJ-17, OBJ-18, OBJ-21	P0	Customer names and other sensitive information must not be revealed