Unencrypted Communication over gRPC

NOM DE VULNÉRABILITÉ	UNENCRYPTED COMMUNICATION OVER GRPC
CWE	CWE-319
Type	**Missing Encryption of Sensitive Data**
Description	The gRPC service communicates in plaintext
Severity	Medium
Impact	Leakage of sensitive data over the network, potential integrity issues
Mitigation	Enable TLS on the gRPC server Remove the --plaintext en production

The gRPC service communicates in plaintext (--plaintext flag) making it vulnerable to network interception and data tampering. This lack of encryption (CWE-319) exposes sensitive data to potential leakage or tampering. Although the severity is medium, it can become critical in sensitive environments. To mitigate this, TLS should be enabled on the gRPC server, and plaintext communication must be disabled in production.

Ryan INGAUTA

Unrestricted SSH Access

VULNERABILITY	UNNECESSARY SSH EXPOSURE
CWE	CWE-668
Type	**Exposure of Resource to Wrong Sphere**
Description	SSH is publicly accessible on a machine primarily intended to serve web content. This increases the attack surface and allows unauthorized access attempts
Severity	Medium
Impact	Unauthorized access, brute-force risk, lateral movement, sensitive data exposure
Mitigation	Restrict SSH to internal/admin IPs, disable password login, use key-based auth, add firewall rules, use a different port, use fail2ban, hide SSH behind VPN or bastion host

The SSH service is unnecessarily exposed on a publicly accessible web server, increasing the attack surface. This corresponds to CWE-668 (Exposure of Resource to Wrong Sphere) and is classified as medium severity. Although not inherently vulnerable, this exposure invites brute-force attempts and can lead to unauthorized access or lateral movement within the network. To mitigate, SSH should be restricted to internal or administrative IPs. Password authentication should be disabled in favor of SSH key-based login. Additional protections can be firewalls, fail2ban, or even changing the default port to reduce visibility.

Ryan INGAUTA

Local Service Exposure

NOM DE VULNÉRABILITÉ	LOCAL SERVICE EXPOSURE WITHOUT AUTHENTICATION
CWE	CWE-306, CWE-1327
Type	**Exposure of Resource to Wrong Sphere, Improper Access Control**
Description	Services were found running on local-only ports (one was listening on 0.0.0.0:8000) without proper authentication or access control. These services are often assumed to be secure just because they are “not exposed,” but once you gain access to the system (via SSH or RCE), they become trivially accessible.
Severity	Medium
Impact	Unauthorized internal access to internal services, leading to a privilege escalation
Mitigation	Enforce authentication and authorization for internal services. Do not bind a service to 0.0.0.0 address . Apply firewall rules to restrict access. Never assume local-only services are inherently secure.

Local services were found on the host with no authentication or access control. While not externally exposed, it becomes fully accessible once local access is gained (e.g., via SSH or RCE). This falls under CWE-306: Missing Authentication for Critical Function. To mitigate, implement authentication for internal services and apply firewall rules. ***Local does not mean secure.***

Weak passwords requirement

VULNERABILITY	WEAK PASSWORDS REQUIREMENT
CWE	CWE-521, CWE-1392, CWE-308
Type	**Use of Weak Credentials**
Description	The system allows the use of weak or default passwords that are easy to guess or crack. This increases the risk of unauthorized access through brute-force or dictionary attacks. Common examples include passwords like “admin,” “password,” or “123456” that are not complex enough to prevent attacks
Severity	High
Impact	Unauthorized access leading to an access to the application/service, brute-force risks
Mitigation	Enforce strong password policies (e.g., minimum length, complexity requirements), implement multi-factor authentication (MFA), enforce account lockout mechanisms after a number of failed attempts, and regularly rotate credentials.

Weak or default passwords, such as "admin" are allowed on the application/services. They are vulnerable to brute-force or dictionary attacks. The system allows weak or default passwords, such as "admin" or "123456," which are vulnerable to brute-force or dictionary attacks. This issue is classified under CWE-521, CWE-1392, and CWE-308 and is of high severity. The impact includes unauthorized access to the application or service. To mitigate, enforce strong password policies, enable multi-factor authentication (MFA), implement account lockouts after failed attempts, and regularly rotate credentials.

Ryan INGAUTA

Remote Code Execution via Vulnerable pyLoad Server

VULNERABILITY	REMOTE CODE EXECUTION VIA VULNERABLE PYLOAD SERVER
CWE	CWE-94, CWE-250
Type	**Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')**
Description	A vulnerability in pyLoad v0.5.0 allows remote attackers to execute arbitrary commands without authentication. The issue exists in the handling of request data before authentication checks are applied
CVE associated	CVE-2023-0297
Severity	Critical (CVSS v3: 9.8)
Impact	Full system compromission
Mitigation	Upgrade pyLoad to a patched version or isolate the service. Prevent exposure of the service to external networks. Implement network segmentation and firewall rules

A Remote Code Execution (RCE) vulnerability in pyLoad v0.5.0 (CVE-2023-0297) allows unauthenticated remote attackers to execute arbitrary commands. This issue arises from improper handling of request data before authentication checks, classified under CWE-94 and CWE-250. The severity is critical (CVSS v3: 9.8), with the potential for full system compromise (root access) . To mitigate, upgrade to a patched pyLoad version, don't run the service with unnecessary privileges, and implement network segmentation with firewall rules to prevent external exposure.

Ryan INGAUTA