Q-SecureScan Report for https://localhost

Generated: 2025-08-26 01:24:13

Summary

Total Items Scanned: 15

High Severity: 4

Medium Severity: 11

Low Severity: 0

Unknown Severity: 0

Compliance Issues: GDPR, PCI-DSS

Scanned Items

Item ID	Type	Protocol/Service	Heuristics	Encryption Markers	Algorithms	Severity	Policy Violations	PQC Recommendation	Remediation Guidance
http	protocol	HTTP	HTTP protocol accessible, no encryption	None	None	High	None	Severity: High; Migrate to HTTPS with quantum-resistant TLS ciphers (e.g., AES-256, CRYSTALS-Kyber)	No remediation required
port_22_tcp	port	ssh	SSH service with cryptographic algorithms; Anomaly: Anomalous item: port_22_tcp	SSH ciphers detected	RSA, ECDSA, ECDH, AES-128, AES-192, AES-256, CHACHA20, SHA1	High	None	Severity: High; Migrate RSA (~0 bits security) to CRYSTALS-Dilithium for signatures or CRYSTALS-Kyber for key exchange at level 1 (e.g., Kyber-512); Severity: High; Migrate ECDSA (~0 bits security) to CRYSTALS-Dilithium at level 1 (e.g., Kyber-512); Severity: High; Migrate ECDH (~0 bits security) to CRYSTALS-Kyber at level 1 (e.g., Kyber-512); Severity: Medium; Migrate AES-128 (~64 bits security) to AES-256 at level 1 (e.g., Kyber-512); Severity: Medium; Migrate AES-192 (~96 bits security) to AES-256 at level 1 (e.g., Kyber-512); Severity: Low; Safe: AES-256 is quantum-resistant; Severity: Low; Safe: CHACHA20 is quantum-resistant; Severity: High; Migrate SHA1 (~80 bits security) to SHA-256 at level 1 (e.g., Kyber-512)	Update SSH configuration to use CRYSTALS-Dilithium for signatures or CRYSTALS-Kyber for key exchange (e.g., `Ciphers aes256-ctr` in sshd_config); Update SSH configuration to use CRYSTALS-Dilithium (e.g., `Ciphers aes256-ctr` in sshd_config); Update SSH configuration to use CRYSTALS-Kyber (e.g., `Ciphers aes256-ctr` in sshd_config); Update SSH configuration to use AES-256 (e.g., `Ciphers aes256-ctr` in sshd_config); Update SSH configuration to use AES-256 (e.g., `Ciphers aes256-ctr` in sshd_config); Update SSH configuration to use SHA-256 (e.g., `Ciphers aes256-ctr` in sshd_config)
port_631_tcp	port	ipp	Open port: ipp	None	None	Medium	None	Severity: Medium; Ensure service uses quantum-resistant algorithms (e.g., AES-256, CRYSTALS-Kyber)	No remediation required
port_3306_tcp	port	nagios-nsca	Open port: nagios-nsca	None	None	Medium	None	Severity: Medium; Ensure service uses quantum-resistant algorithms (e.g., AES-256, CRYSTALS-Kyber)	No remediation required
port_4369_tcp	port	epmd	Open port: epmd	None	None	Medium	None	Severity: Medium; Ensure service uses quantum-resistant algorithms (e.g., AES-256, CRYSTALS-Kyber)	No remediation required
port_5432_tcp	port	postgresql	TLS-enabled service	TLS ciphers detected	RSA-2048, DH-2048, RSA	High	None	Severity: High; Migrate RSA-2048 (~113 bits security) to CRYSTALS-Dilithium for signatures or CRYSTALS-Kyber for key exchange at level 1 (e.g., Kyber-512); Severity: High; Migrate DH-2048 (~113 bits security) to CRYSTALS-Kyber at level 1 (e.g., Kyber-512); Severity: High; Migrate RSA (~0 bits security) to CRYSTALS-Dilithium for signatures or CRYSTALS-Kyber for key exchange at level 1 (e.g., Kyber-512)	Configure postgresql to use CRYSTALS-Dilithium for signatures or CRYSTALS-Kyber for key exchange (e.g., set `SSLCipherSuite ECDHE-RSA-AES256-GCM-SHA384` in web server config); Configure postgresql to use CRYSTALS-Kyber (e.g., set `SSLCipherSuite ECDHE-RSA-AES256-GCM-SHA384` in web server config); Configure postgresql to use CRYSTALS-Dilithium for signatures or CRYSTALS-Kyber for key exchange (e.g., set `SSLCipherSuite ECDHE-RSA-AES256-GCM-SHA384` in web server config)
port_5672_tcp	port	amqp	Open port: amqp	None	None	Medium	None	Severity: Medium; Ensure service uses quantum-resistant algorithms (e.g., AES-256, CRYSTALS-Kyber)	No remediation required
port_5939_tcp	port	unknown	Open port: unknown	None	None	Medium	None	Severity: Medium; Ensure service uses quantum-resistant algorithms (e.g., AES-256, CRYSTALS-Kyber)	No remediation required
port_6379_tcp	port	redis	Open port: redis	None	None	Medium	None	Severity: Medium; Ensure service uses quantum-resistant algorithms (e.g., AES-256, CRYSTALS-Kyber)	No remediation required
port_7070_tcp	port	realserver	TLS-enabled service	TLS ciphers detected	RSA-2048, DH-2048, 3DES, RSA	High	3DES violates Weak Ciphers in realserver	Severity: High; Migrate RSA-2048 (~113 bits security) to CRYSTALS-Dilithium for signatures or CRYSTALS-Kyber for key exchange at level 1 (e.g., Kyber-512); Severity: High; Migrate DH-2048 (~113 bits security) to CRYSTALS-Kyber at level 1 (e.g., Kyber-512); Severity: High; Migrate 3DES (~56 bits security) to AES-256 at level 1 (e.g., Kyber-512); Severity: High; Migrate RSA (~0 bits security) to CRYSTALS-Dilithium for signatures or CRYSTALS-Kyber for key exchange at level 1 (e.g., Kyber-512)	Configure realserver to use CRYSTALS-Dilithium for signatures or CRYSTALS-Kyber for key exchange (e.g., set `SSLCipherSuite ECDHE-RSA-AES256-GCM-SHA384` in web server config); Configure realserver to use CRYSTALS-Kyber (e.g., set `SSLCipherSuite ECDHE-RSA-AES256-GCM-SHA384` in web server config); Configure realserver to use AES-256 (e.g., set `SSLCipherSuite ECDHE-RSA-AES256-GCM-SHA384` in web server config); Configure realserver to use CRYSTALS-Dilithium for signatures or CRYSTALS-Kyber for key exchange (e.g., set `SSLCipherSuite ECDHE-RSA-AES256-GCM-SHA384` in web server config)
port_11434_tcp	port	unknown	Open port: unknown	None	None	Medium	None	Severity: Medium; Ensure service uses quantum-resistant algorithms (e.g., AES-256, CRYSTALS-Kyber)	No remediation required
port_15672_tcp	port	unknown	Open port: unknown	None	None	Medium	None	Severity: Medium; Ensure service uses quantum-resistant algorithms (e.g., AES-256, CRYSTALS-Kyber)	No remediation required
port_25672_tcp	port		Open port:	None	None	Medium	None	Severity: Medium; Ensure service uses quantum-resistant algorithms (e.g., AES-256, CRYSTALS-Kyber)	No remediation required
port_27017_tcp	port	mongodb	Open port: mongodb	None	None	Medium	None	Severity: Medium; Ensure service uses quantum-resistant algorithms (e.g., AES-256, CRYSTALS-Kyber)	No remediation required
port_33060_tcp	port	mysqlx	Open port: mysqlx	None	None	Medium	None	Severity: Medium; Ensure service uses quantum-resistant algorithms (e.g., AES-256, CRYSTALS-Kyber)	No remediation required

Skipped Items

Item: https://localhost:443: Port 443 closed