Spice Labs

Post-Quantum Cryptography Security Report

Survey Tag: API Gateway

Survey Date: January 15, 2025

Report Date: November 12, 2025

This report was generated by **Spice Labs Topographer**, which surveys your deployment artifacts using cryptographic analysis to identify quantum-vulnerable algorithms and reveal your true cryptographic security posture. For more information, visit www.spicelabs.io

Table of Contents

Executive Summary

BANNED ALGORITHMS:

2

NEEDS ATTENTION:

MIXED CRYPTOGRAPHY

2

TRANSITION AWAY (BY 2030)

2

POST-QUANTUM READY:

1

Critical: Banned Algorithms

These libraries use cryptographic algorithms that are broken and can be cracked using conventional computers today (RC2, RC4, DES, 3DES, MD5, SHA-1, RSA-1024, etc.).

▼ `legacy-rsa` v1.2.3

Package URL

`pkg:maven/com.sun.security/legacy-rsa@1.2.3`

Cryptographic Algorithms

RSA-1024 (Asymmetric Encryption) BANNED

SHA-1 (Hash Function) BANNED

Found in Files

`com/sun/security/auth/RSAEncryption.class`

`com/sun/security/crypto/CipherUtil.class`

Assessment

> This library uses RSA-1024 and SHA-1, both of which are explicitly banned due to known vulnerabilities to quantum attacks. RSA-1024 can be broken by Shor's algorithm, and SHA-1 has collision vulnerabilities. Immediate migration required.

▼ `LegacyCrypto.Utilities` v2.1.0

Package URL

`pkg:nuget/LegacyCrypto.Utilities@2.1.0`

Cryptographic Algorithms

DES (Symmetric Encryption) BANNED

MD5 (Hash Function) BANNED

Found in Files

`LegacyCrypto.Utilities.dll`

Assessment

Contains DES and MD5 which are cryptographically broken. These algorithms offer no security against modern attacks and are trivially breakable with quantum computers.

Warning: Mixed Cryptography

These libraries contain both post-quantum safe and legacy cryptographic algorithms. Migration to post-quantum only is recommended.

▼ bcprov-jdk18on v1.78

Package URL

`pkg:maven/org.bouncycastle/bcprov-jdk18on@1.78`

Cryptographic Algorithms

- **SPHINCS+** (Digital Signature) — POST-QUANTUM
- **RSA-2048** (Asymmetric Encryption) — LEGACY
- **ECDSA-P256** (Digital Signature) — LEGACY
- **AES-256-GCM** (Symmetric Encryption) — LEGACY

Found in Files

- `org/bouncycastle/pqc/crypto/sphincsplus/SPHINCSPlusEngine.class`
- `org/bouncycastle/crypto/engines/RSABlindedEngine.class`
- `org/bouncycastle/crypto/signers/ECDSASigner.class`
- `org/bouncycastle/crypto/engines/AESEngine.class`

Assessment

BouncyCastle's main provider library includes some post-quantum algorithms (SPHINCS+) alongside traditional cryptography (RSA-2048, ECDSA-P256, AES-256-GCM) for backward compatibility. While the post-quantum signatures are quantum-resistant, the legacy RSA and ECDSA components remain vulnerable to Shor's algorithm. Migration to bcpqc-jdk18on (pure post-quantum) is recommended.

▼ BouncyCastle.Cryptography v2.4.0

Package URL

`pkg:nuget/BouncyCastle.Cryptography@2.4.0`

Cryptographic Algorithms

LMS (Hash-Based Signature)	POST-QUANTUM
RSA-4096 (Asymmetric Encryption)	LEGACY
ECDH-P384 (Key Exchange)	LEGACY

Found in Files

`BouncyCastle.Cryptography.dll`

Assessment

The .NET port of BouncyCastle includes Leighton-Micali Signatures (LMS), a hash-based post-quantum signature scheme, but maintains extensive legacy cryptography for compatibility. RSA-4096 and elliptic curve algorithms (ECDH P-384) remain quantum-vulnerable. Consider migrating to pure post-quantum alternatives as application requirements allow.

Transition Away: Deprecated by 2030

These libraries use cryptographic algorithms that are being deprecated by 2030 under NIST IR 8547. This includes AES-128, RSA (>1024 bits), and Elliptic Curve algorithms. Plan migration to post-quantum alternatives.

▾ openssl v3.0.2-0ubuntu1.15

Package URL

`pkg:deb/ubuntu/openssl@3.0.2-0ubuntu1.15`

Cryptographic Algorithms

RSA-2048 (Asymmetric Encryption)	TRANSITION
ECDSA-P256 (Digital Signature)	TRANSITION
AES-128-CBC (Symmetric Encryption)	TRANSITION

Found in Files

- `/usr/lib/x86_64-linux-gnu/libssl.so.3`
- `/usr/lib/x86_64-linux-gnu/libcrypto.so.3`

Assessment

> OpenSSL 3.0 includes RSA-2048, ECDSA on P-256 curves, and AES-128 which are being deprecated by 2030 under NIST IR 8547. While currently secure against classical attacks, these algorithms are vulnerable to quantum attacks. Begin planning migration to post-quantum alternatives like Kyber for key exchange and Dilithium for signatures.

▾ libgcrypt20 v1.10.1-3ubuntu2

Package URL

`pkg:deb/ubuntu/libgcrypt20@1.10.1-3ubuntu2`

Cryptographic Algorithms

ECC-Curve25519 (Key Exchange)	TRANSITION
RSA-3072 (Asymmetric Encryption)	TRANSITION
AES-128-GCM (Symmetric Encryption)	TRANSITION

Found in Files

```
/usr/lib/x86_64-linux-gnu/libgcrypt.so.20
```

Assessment

Libgcrypt implements elliptic curve cryptography (Curve25519), RSA-3072, and AES-128 which will be phased out by 2030. These algorithms provide strong classical security but are quantum-vulnerable. The 2030 deadline under NIST IR 8547 requires transitioning to post-quantum cryptography such as Kyber-1024 and ChaCha20-Poly1305.

Compliant: Post-Quantum Ready

These libraries use 100% post-quantum safe cryptographic algorithms and are ready for the quantum computing era.

▼ bcpqc-jdk18on v1.77

Package URL

`pkg:maven/org.bouncycastle/bcpqc-jdk18on@1.77`

Cryptographic Algorithms

Kyber-1024 (Key Encapsulation)	POST-QUANTUM
Dilithium-5 (Digital Signature)	POST-QUANTUM
SPHINCS+ (Digital Signature)	POST-QUANTUM

Found in Files

- `org/bouncycastle/pqc/crypto/kyber/KyberKEMGenerator.class`
- `org/bouncycastle/pqc/crypto/dilithium/DilithiumSigner.class`
- `org/bouncycastle/pqc/crypto/sphincsplus/SPHINCSPlusEngine.class`

Assessment

Fully compliant post-quantum cryptography library. Uses NIST-standardized algorithms (Kyber-1024, Dilithium-5) that are resistant to both classical and quantum attacks. No migration needed.