20TH ANNIVERSARY EDITION

WSO2CON ASIA

PLATFORMLESS MODERNIZATION

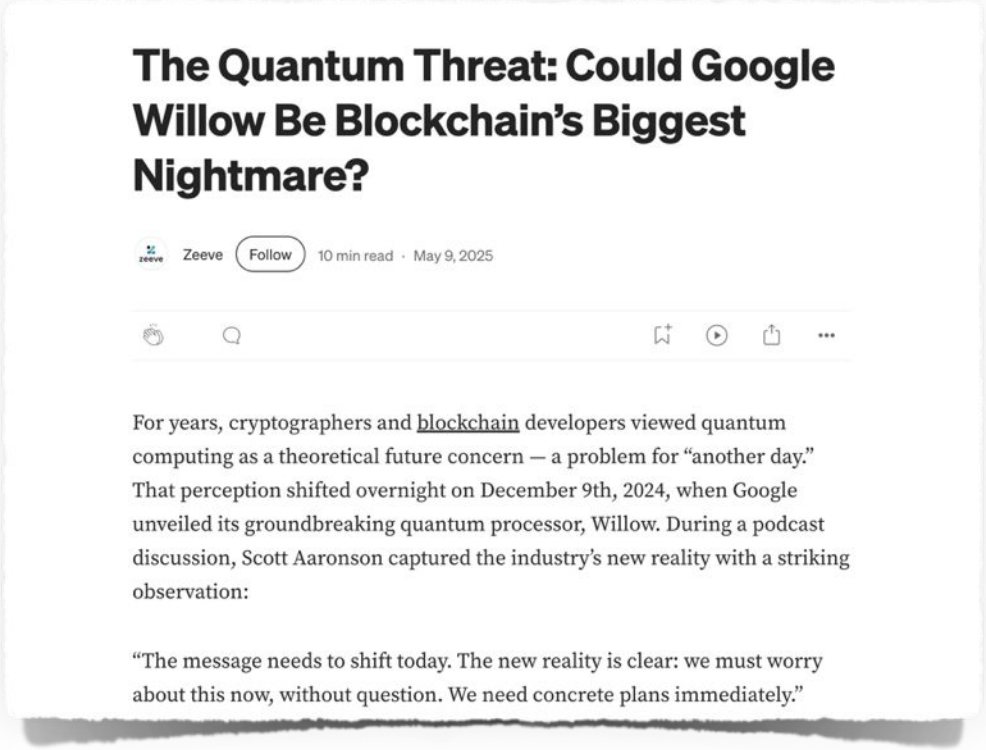
Quantum Threats are closer than you think!

Dr. Frank LEYMANN - Technical Fellow

Isabelle MAUNY - Field CTO

WSO2

Q-DAY is getting closer!



The Quantum Threat: Could Google Willow Be Blockchain's Biggest Nightmare?

Zeeve Follow 10 min read · May 9, 2025

For years, cryptographers and blockchain developers viewed quantum computing as a theoretical future concern — a problem for "another day." That perception shifted overnight on December 9th, 2024, when Google unveiled its groundbreaking quantum processor, Willow. During a podcast discussion, Scott Aaronson captured the industry's new reality with a striking observation:

"The message needs to shift today. The new reality is clear: we must worry about this now, without question. We need concrete plans immediately."

IBM

IBM Institute for Business Value Our insights C-suite Study Hybrid by Design Generative

5 mindshifts to supe

Home / Quantum computing / The quantum clock is ticking: How quantum safe is your organization?

The quantum clock is ticking: How quantum safe is your organization?

In partnership with GSMA, we explore why quantum-safe computing and cybersecurity must become board-level considerations.

Why Should You Worry **NOW** ?

age Credit: https://pixabay.com/photos/man-portrait-model-beard-5891109/

Quantum Computing Can Break RSA With Fewer Qubits Than Previously Known

Published On: June 3, 2025 By James Maguire

In a serious warning for industries relying on current encryption standards, a new research paper by Google Quantum AI reveals that breaking RSA encryption requires far less quantum compute power than widely believed. The paper's findings are a wakeup call to cybersecurity professional to develop quantum-safe security technologies.

The research paper, whose lead author is Google quantum research scientist Craig Gidney, reflects quantum computing's rapid progress over the last five years. "We published a preprint demonstrating that 2048-bit RSA encryption could theoretically be broken by a quantum computer with 1 million noisy qubits running for one week," Gidney wrote. Remarkably, he noted, this is a 20-fold decrease in the number of qubits from the number required in a paper he co-authored in 2019.

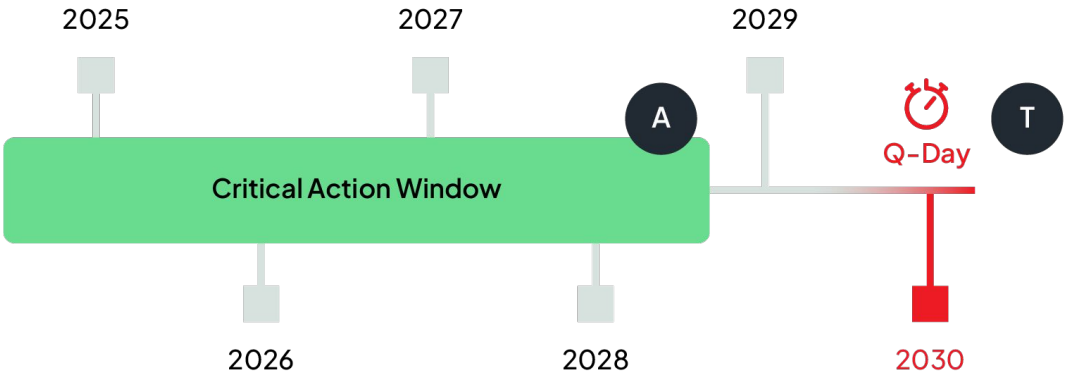
It has started!

QUANTUM SECURITY

Shor's Algorithm Breaks 5-bit Elliptic Curve Key on 133-Qubit Quantum Computer

July 17, 2025
BY QUANTUM NEWS

Harvest now, decrypt later



R

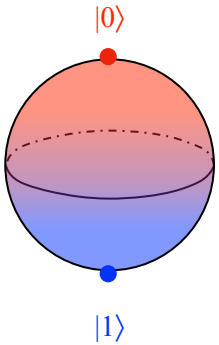
Industry **Data Retention** Periods (R)

- Commercial Data
- Tax Records
- Financial / Banking Records
- Government Records
- Mortages

If (Retention Period + Action time) > T
Your data can be compromised

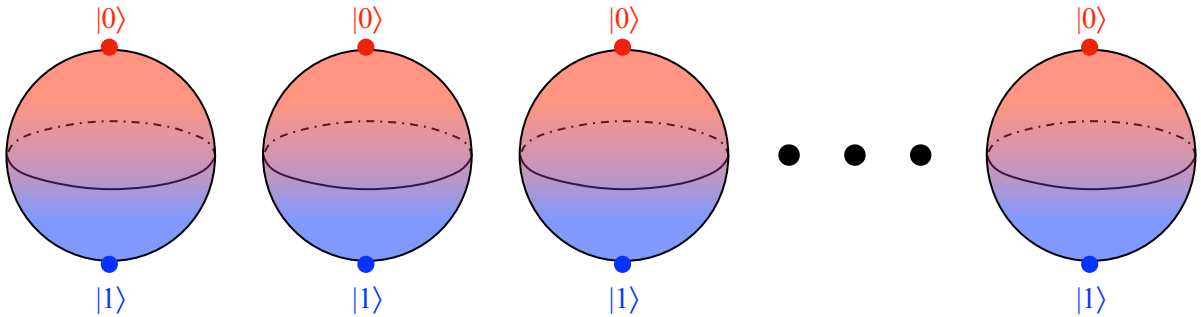
Quantum 101 : the power of a single quantum bit

Bit



Qubit

Quantum 101: The Power of a Quantum Register



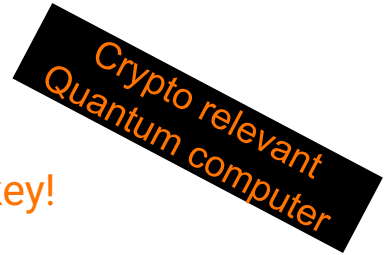
n qubits ⇒ superposition of values at the same time

#atoms in universe $\leq \mapsto n$=300 Qbits

Quantum Parallelism

Why are quantum computers good at cracking RSA?

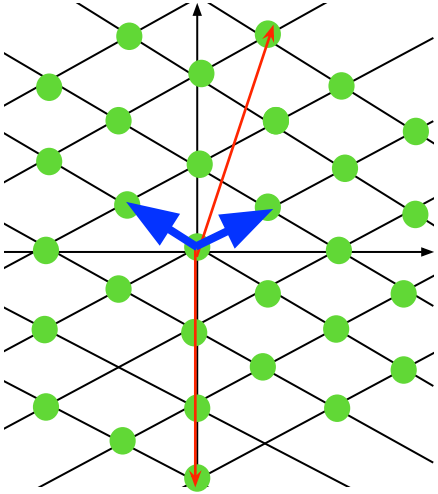
- With RSA, the private key **is the product of two large prime numbers**
- Computing factors of N can be reduced to determine period of function
  - i.e. compute the "discrete logarithm”

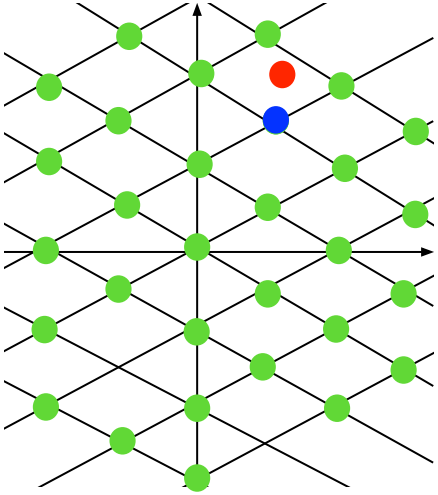


- A quantum computer could derive the private key from the public key!

- Other algorithms like ECC can also be cracked.

Lattice-Based Crypto to the rescue...



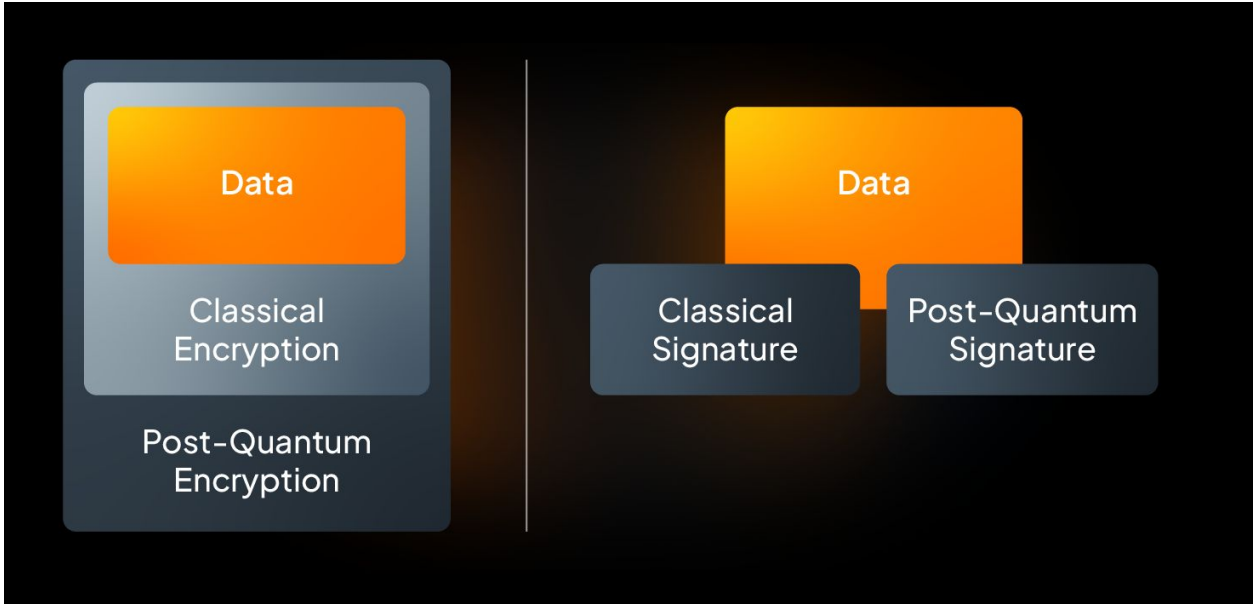


"Learning with Errors"

NIST Standards: ML-KEM (Kyber), ML_DSA (Dilithium)

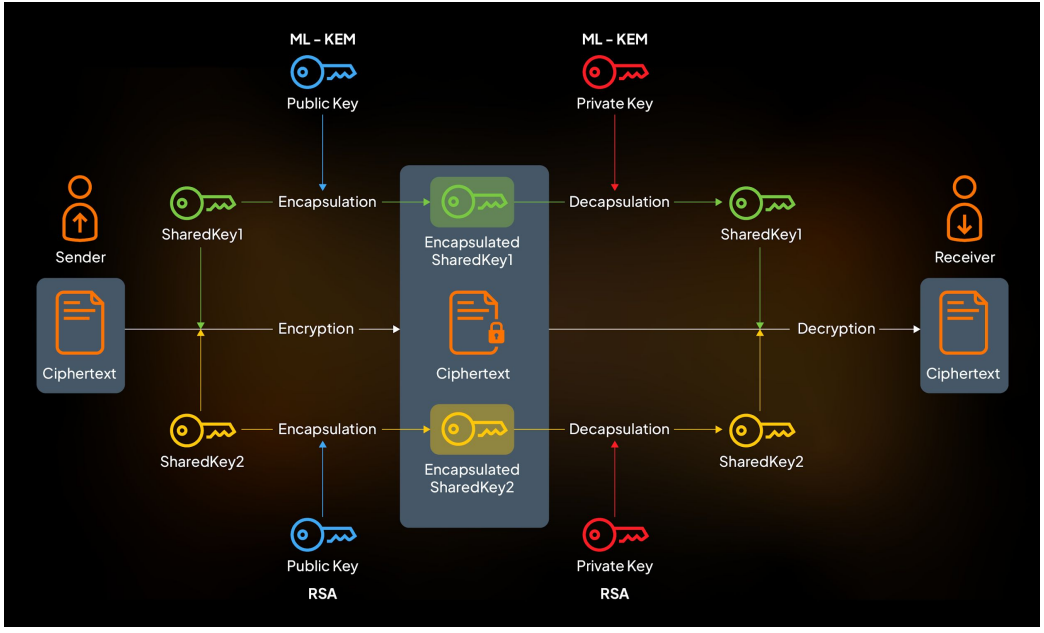
Dual Algorithms approach

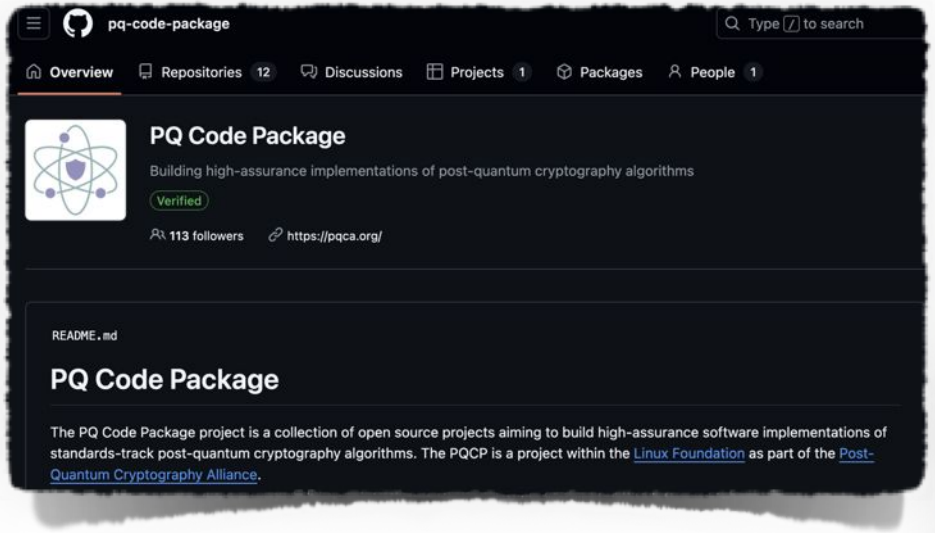
- Post-quantum algorithms (Q) are gradually gaining prominence but require time to establish trust within the industry
- Need for dual approach



Using Hybrid Key Encryption

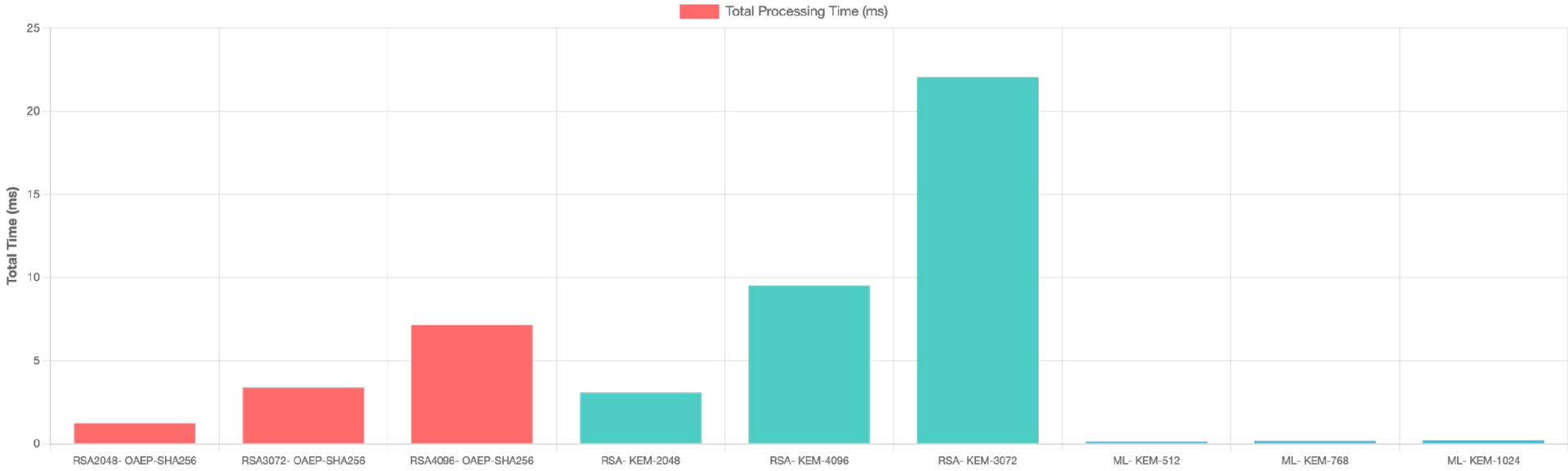
- Combines the conventional RSA-KEM with the post-quantum ML-KEM-768 (approved by NIST)
- Allows you to start to be prepared now!



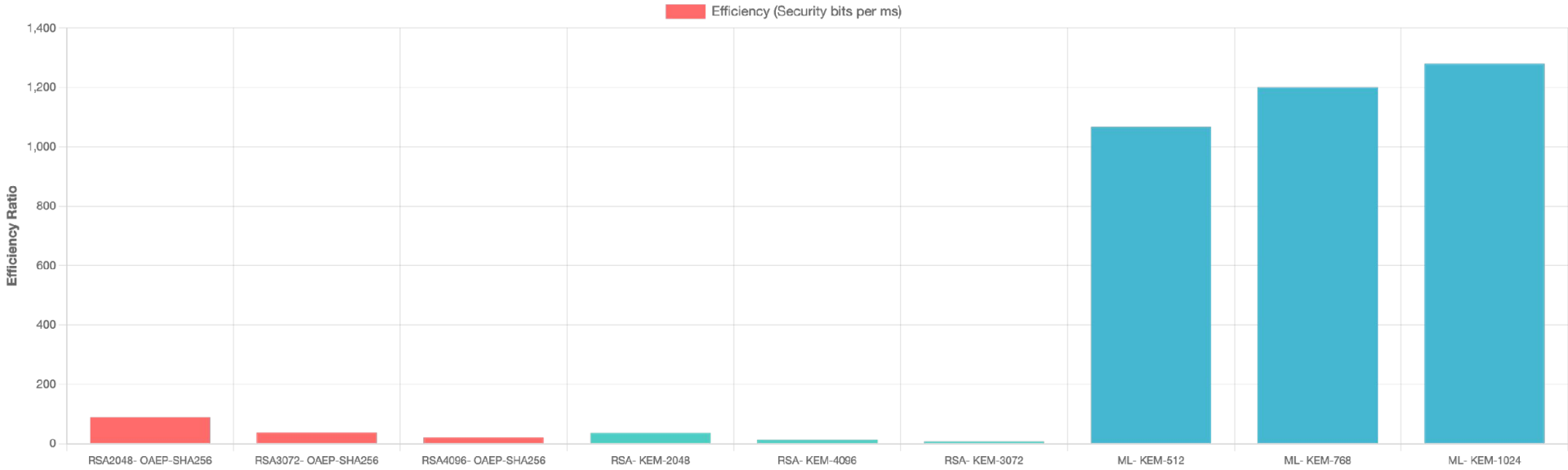


All algorithms are Open Source!

Quantum-resistant doesn't mean slow!



ML-KEM is the clear winner for performance vs. security ratio!



Google Chrome Switches to ML-KEM for Post-Quantum Cryptography Defense

Sep 17, 2024 Ravie Lakshmanan Browser Security / Quantum Computing

Google has announced that it will be switching from KYBER to ML-KEM in its Chrome web browser as part of its ongoing efforts to defend against the risk posed by cryptographically relevant quantum computers (CRQCs).

"Chrome will offer a key share prediction for hybrid ML-KEM (codepoint 0x11EC)," David Adrian, David Benjamin, Bob Beck, and Devon O'Brien of the Chrome Team said. "The PostQuantumKeyAgreementEnabled flag and enterprise policy will apply to both Kyber and ML-KEM."

— Most Read News


New PumaBot Botnet Targets Linux IoT Devices to Steal SSH Credentials and Mine Crypto

Researchers Expose New Intel CPU Flaws Enabling Memory Leaks and Spectre v2 Attacks


Hackers Use TikTok Videos to Distribute Vidar and StealC Malware via ClickFix Technique

AWS Default IAM Roles Found to Enable Lateral Movement and Cross-Service Exploitation


Critical Windows Server 2025 dMSA Vulnerability Enables Active Directory Compromise

Russian Hackers Breach 20+ NGOs Using Evilginx Phishing via Fake Microsoft Entra Pages

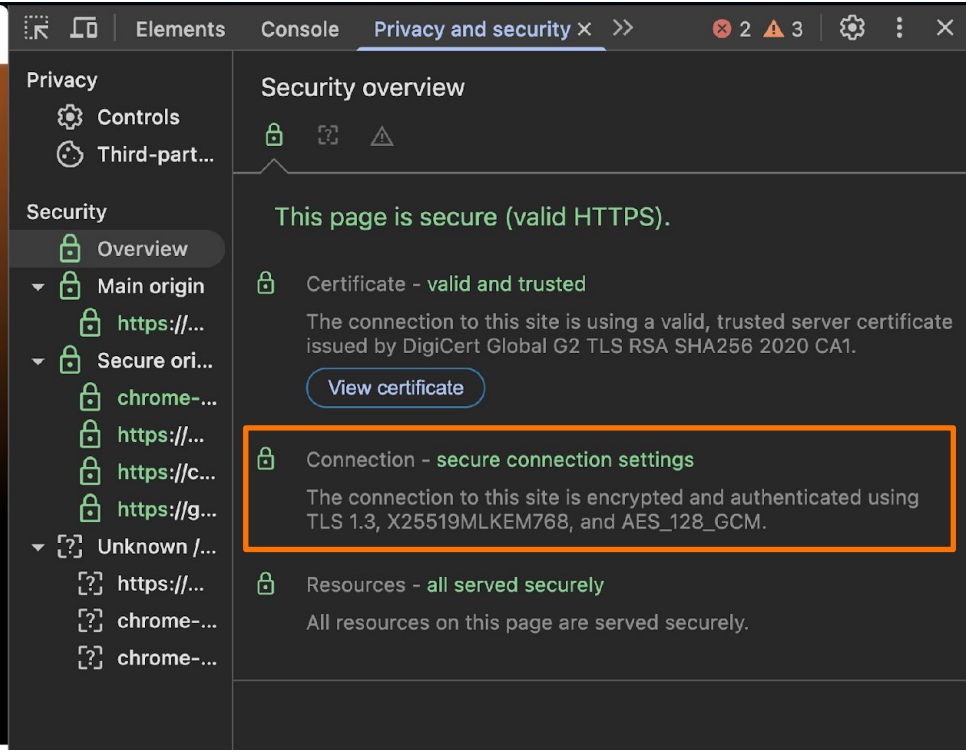
More Stories ▼

WSO2

The Future of Internet Security: Preparing for the Post-Quantum Era

The global IT security infrastructure relies on private-public key mechanisms such as RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography). These mechanisms face a significant threat from the development of quantum computers.

Over the next few years, quantum computers will possess sufficient computational power to break encryption based on these algorithms. For instance, while classical algorithms would require the age of the universe to factor an RSA 2048 key, a sufficiently powerful quantum computer could potentially achieve this in a matter of hours.



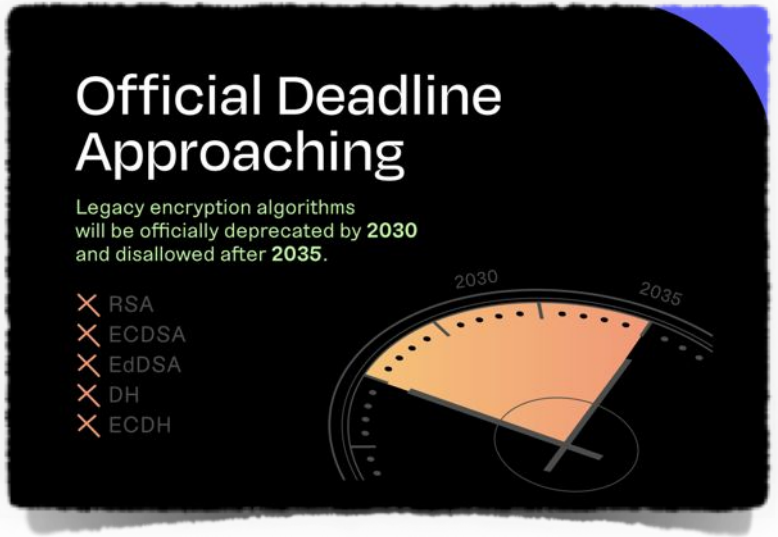
Regulations

Public Law 117 - 260 - Quantum Computing Cybersecurity Preparedness Act

Summary | Related Documents

Category	Bills and Statutes
Collection	Public and Private Laws
SuDoc Class Number	AE 2.110:117-260
Law Number	Public Law 117-260
Date Approved	December 21, 2022
Full Title	An act to encourage the migration of Federal Government information technology systems to quantum-resistant cryptography, and for other purposes.
Bill Number	H.R. 7535
Report Number	S Rept. 117-251
Statutes at Large Citations	136 Stat. 2389, 2390, 2391 and 2392
United States Code Citations	44 U.S.C. 3502, 3552 and 3553 Chapter 35
Legislative History	LEGISLATIVE HISTORY–H.R. 7535 (S. 4592):

NIS2



EUROPEAN COMMISSION

Brussels, 11.4.2024
C(2024) 2393 final

COMMISSION RECOMMENDATION

of 11.4.2024

on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

CSF 2.0

WSO2 and Post Quantum Support

- The Ballerina language is post quantum ready !
  - Supports signatures and encryption using combined standard and PQC algorithms
- WSO2 Identity Server also supports Post Quantum algorithms
- More to come!

Questions Time!


Thank you!
20TH ANNIVERSARY EDITION
WSO2CONASIA
PLATFORMLESS MODERNIZATION