Rahbar International

Thursday, October 16th 2025

OIC-CERT & Huawei release framework to secure software supply chains across member states

Published on January 31, 2025

Document Date: Thu, Oct 16 2025 01:34:03 pm

Category: ,English,Qatar - ,Snippets

Show on website : Click Here

Doha-Qatar 29 January 2025 – Huawei, in collaboration with the Organization of the Islamic Cooperation-Computer Emergency Response Team (OIC-CERT) and the Oman National CERT, today announced the release of the OIC-CERT Software Supply Chain Security Framework. This framework provides crucial guidance to OIC member states on establishing robust software supply chain security management, ensuring end-to-end cybersecurity. This comes at a critical time when cybersecurity is a top priority for businesses in the region, with 55% of companies in the

Middle East prioritizing mitigating digital and technology risks over the next year, exceeding the global average of 53%, according to a report by PwC. Within this, cyber risks remain a significant concern, with 42% of regional businesses focusing on them.

Developed by the OIC-CERT Supply Chain Security working group, co-chaired by the Oman National CERT and Huawei, the framework addresses the growing complexity and interconnectedness of software systems and the increasing risks of supply chain attacks. It offers practical guidance for regulatory authorities in member countries to formulate effective policies for software supply chain manufacturers and service providers.

The framework provides a comprehensive approach to software supply chain security governance, covering key areas such as supplier cybersecurity management, open-source software management, R&D and production management. It guides organizations in implementing security measures throughout the entire software lifecycle, from evaluating and selecting suppliers to securing the development and deployment processes. It also emphasizes the importance of managing open-source software components and integrating security practices into research, development, and production environments. This holistic approach aims to mitigate risks throughout the software supply chain.

Aloysius Cheang, Chief Security Officer for Huawei in the Middle East and Central Asia, said: "Huawei is committed to collaborating with global partners to enhance cybersecurity for all. This framework represents a significant step forward in strengthening software supply chain security across the OIC member states. We believe that by working together and sharing best practices, we can create a more secure and trustworthy digital environment for everyone."

Dr. Saleh Said Al Hashmi at Oman National CERT, highlighted the significance of this framework and the value of collaboration, stating: "In today's interconnected world, software supply chain security is paramount. This framework provides a crucial foundation for OIC member states to build resilient digital economies. Our collaboration with Huawei leverages their expertise and industry insights to develop comprehensive guidelines that address the evolving threat landscape. By adopting these recommendations, nations can effectively mitigate risks and protect critical infrastructure. We believe this joint effort will significantly enhance cybersecurity across the OIC community."

The framework's release comes at a pivotal moment, as software supply chain attacks continue to evolve and pose significant threats to organizations and nations. By prioritizing supply chain

cybersecurity, OIC member states can protect their digital assets, foster trust, and enhance resilience in an increasingly interconnected world.

This initiative underscores Huawei's ongoing commitment to contributing to the development of cybersecurity standards and enhancing industry security capabilities. By collaborating with international organizations like OIC-CERT, Huawei aims to support the building of cyber resilience and contribute to a more secure and trustworthy cyberspace.