CWNP Unveils New Whitepaper on WPA2 Vulnerabilities and the Transition to WPA3

Durham, North Carolina Jan 17, 2026 (Issuewire.com**)** - CWNP, the global leader in vendor-neutral wireless LAN certification, has long been at the forefront of educating IT professionals in wireless networking technologies. Today, CWNP explores the evolution of wireless security from WEP to WPA2 and the growing importance of transitioning to WPA3 in response to modern security challenges. In their newly released whitepaper, ***"Revisiting WPA2: Understanding Its Security Gaps and Evaluating the Move to WPA3, by Iftikhar Javed Khan"*** the author delves deeper into these topics, offering insights into the risks associated with WPA2 and providing actionable steps for organizations to adopt WPA3 for enhanced security.

Wireless networks are ubiquitous, becoming the standard for connectivity in homes, businesses, and critical infrastructures worldwide. Since its introduction in the early 2000s, WPA2 has served as the backbone of wireless security, providing confidentiality, access control, and data integrity. However, as cyber threats evolve, WPA2 has shown vulnerabilities that cannot be ignored.

The 2017 KRACK attacks and 2018 PMKID hash vulnerability exposed significant weaknesses in WPA2. These discoveries have led to an industry-wide conversation about the transition to WPA3, the next-generation security protocol designed to address WPA2's shortcomings. However, adopting WPA3 requires careful consideration due to the complexity of infrastructure upgrades and ongoing vulnerabilities, including those related to downgrade and side-channel attacks.

At CWNP, we understand that no single solution fits all environments. Organizations around the world continue to evaluate the most effective ways to protect their wireless networks, whether through

patching existing WPA2 systems, transitioning to WPA3, or a combination of both. As of today, an estimated 20–30 percent of devices using WPA2 remain unpatched, highlighting the need for proactive action.

Key Highlights of the Paper:

- **The Evolution of Wireless Security**: From WEP's inception to WPA2's widespread use, and the potential of WPA3.
- **Vulnerabilities in WPA2**: Insights into the PMKID Hash Dictionary Attack and the KRACK vulnerability, and their impact on wireless security.
- **WPA3 Enhancements**: A detailed look at WPA3's improved features, including Simultaneous Authentication of Equals (SAE), Protected Management Frames (PMF), and Operating Channel Validation (OCV).
- **Practical Recommendations**: Mitigation strategies for organizations still relying on WPA2, including firmware updates, Intrusion Detection Systems (IDS), and targeted countermeasures.
- **The Path Forward**: As enterprises look to secure their wireless networks, CWNP offers guidance on making informed decisions for a seamless transition to WPA3.

"Wireless security is no longer just about protecting data; it's about protecting the very infrastructure that organizations rely on," said Tom Carpenter, Director at CWNP. "As the wireless industry advances, it's critical that professionals are equipped with the knowledge and tools to stay ahead of emerging threats. Our certification programs continue to focus on providing in-depth knowledge of these technologies, preparing the next generation of wireless experts."

CWNP’s comprehensive certification programs prepare IT professionals to design, implement, and manage enterprise wireless networks with a focus on security. With over 150 countries participating in our training and certification programs, CWNP is proud to be a trusted partner for individuals and organizations striving to maintain secure, reliable wireless networks.

About CWNP
Founded in 1999, CWNP is the world’s leading provider of vendor-neutral wireless LAN certification programs. Our certifications cover the entire spectrum of wireless technologies, equipping professionals with the expertise to work with all enterprise WLAN products. CWNP has certified professionals in more than 150 countries, helping organizations deploy cost-effective, reliable, and secure wireless LANs. To learn more, visit https://www.cwnp.com/

For more information or media inquiries, please contact:
Kate McCall
Director of Marketing
Certitrek Group / CWNP
marketing@certitrek.com

Media Contact

CWNP (Certified Wireless Network Professional)

*********@certitrek.com

8664382963

2222 Sedwick Rd

Source : CWNP (Certified Wireless Network Professional)

See on IssueWire