WP2C Wi-Fi Network Security Report

Report Generated on: 2023-03-09 15:55:30

Network Name:	C208
Mac Address:	58:D5:6E:A1:21:A6
Encryption:	WPA
Password:	huatAR777
Handshake Captured Date and Time:	2023-03-09 13:33:01
Cracked Date and Time:	2023-03-09 15:55:30

Password Vulnerabilities:

1. Password Strength: Medium (3/4)
2. Estimated number needed to guess the password: 100010000
3. Estimated time needed to guess the password (offline fast hashing with many processors): less than a second
4. Estimated time needed to guess the password (offline slow hashing with many processors): 3 hours
5. Estimated time needed to guess the password (online attack without throttling): 4 months
6. Estimated time needed to guess the password (online attack with throttling): centuries

Password Exposure:

zxcvbn: No matches found.

WP2C: huatAR777 found in for_passphases at position 1.

WP2C: huatAR777 found in probable at position 257659.

Comments and Recommendations for Weak Password:

None

Recommendations to Avoid WPA Vulnerabilities:

1. Use WPA3 instead of WPA2
2. Use a strong, unique password for your Wi-Fi network
3. Regularly update the firmware of your Wi-Fi router
4. Disable WPS (Wi-Fi Protected Setup)
5. Disable legacy Wi-Fi protocols (e.g. 802.11b)
6. Avoid using dictionary words in your password
7. Use a combination of uppercase and lowercase letters, numbers, and symbols
8. Use a longer password, at least 12 characters
9. Change your password regularly
10. Consider using a password manager to generate and store strong passwords
11. Use WPA3 or WPA2 with AES encryption instead of WEP, which is vulnerable to attacks