Carson City

Wireless Assessment – Summary Report

April 2022

Submitted By:

Nathan Kramer – CEH
Senior Threat Management Consultant

Michael Nouguier – CISSP, PMP
Director, Cybersecurity Services

EideBailly

CYBERSECURITY SOLUTIONS

Overview

Carson City contracted Eide Bailly to conduct a Wireless Assessment. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against the organization. The goal of the Wireless Assessment was to identify what vulnerabilities are present throughout Carson City's wireless networks.

Efforts were placed on identifying and exploiting security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The assessment was conducted with the level of access that a guest user would have. The assessment was conducted following industry best practices and standards, with all tests and actions being conducted under controlled conditions.

This report documents the Wireless Assessment performed on Carson City's wireless networks, conducted from April 25 to April 28, 2022.

Scope

The scope of this assessment was limited to Carson City's wireless networks and infrastructure as well as publicly available information. Eide Bailly tested the wireless networks in both the Carson City City Hall and Carson City Courthouse.

Summary of Results

Based on the testing performed, Eide Bailly determined that Carson City properly segments its wireless networks by using an open guest network that is separate from its secured corporate networks. None of the networks identified within scope had WPS or other vulnerable extensions enabled. Eide Bailly found that all of Carson City's secured networks are using WPA2. This protocol is the approved Wi-Fi Alliance interoperable implementation of the IEEE 802.11i security standard. Eide Bailly also noted that Carson City's wireless networks use the MGT-CCMP encryption mechanism, which is the security standard used with WPA2 wireless networks.

Additionally, Carson City's wireless networks require both a username and password in order to successfully authenticate and obtain network access. By requiring a username and password combination, rather than simply requesting only a password, Carson City implements an extra layer of wireless network security.

Overall, Eide Bailly identified **one (1) low-risk** finding throughout the Wireless Assessment. This issue was brought to the Carson City IT team immediately and **the issue was remediated.**

The technical details of this assessment's results, including a full technical writeup of the testing performed, have been obfuscated from this report for security purposes. A version of this report that includes those details was provided to Carson City's Technology team in April of 2022.

About Eide Bailly

Eide Bailly advocates penetration testing for impact instead of penetration testing for coverage. Penetration testing for coverage has risen in popularity in recent years as a simplified assessment method used in situations where the goal is to meet regulatory needs. As a form of vulnerability scanning, penetration testing for coverage includes selective verification of discovered issues through exploitation, allowing service providers to conduct the work mainly through automated toolsets and maintain product consistency across multiple engagements.

Penetration testing for impact is a form of attack simulation under controlled conditions, which closely mimics the real-world, targeted attacks that organizations face on a day-to-day basis. Penetration testing for impact is a goal-based assessment, which creates more than a simple vulnerability inventory instead of providing the true business impact of a breach. An impact-based penetration test identifies areas for improvement that will result in the highest rate of return for the business.

Penetration testing for impact poses the challenge of requiring a high skill set to complete. As demonstrated in this report, Eide Bailly believes that it is uniquely qualified to deliver world-class results when conducting penetration tests for impact due to the level of expertise found within our team of security professionals.

Eide Bailly offers a product that cannot be matched in the market. However, we may not be the right fit for every job. Eide Bailly typically conducts consulting services with a low volume, high skill ratio to allow Eide Bailly staff to more closely mimic real-world situations, enabling customers to have increased access to industry-recognized expertise, all while keeping costs reasonable. High volume/fast turn-around engagements are often not a good fit for our services. Eide Bailly is focused on conducting high-quality, high-impact assessments and actively seeks out customers in need of services that other vendors cannot deliver.

If you would like to discuss your penetration testing needs, please contact us at khendrickson@eidebailly.com.