Carson City

Retest – 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 an Internal Vulnerability Assessment and External Penetration Test. These assessments were conducted from September 14 to October 1, 2020. After completing these assessments and delivering the Final Reports, Carson City had the opportunity to remediate the identified vulnerabilities. Eide Bailly then performed a retest of the vulnerabilities from April 25 to April 28, 2022, and aimed to examine the effectiveness of Carson City's remediation activities.

Eide Bailly highly recommends performing a retest after an initial assessment is complete and the organization has been able to remediate any identified issues. Retesting attempts to reproduce each vulnerability to validate remediation activities were successful. Penetration Test and Vulnerability Assessment Retests can provide many benefits to your organization, including:

- Demonstration of your organization's commitment to security
- Decreased mean time to remediation (MTTR) due to defined windows of retest
- Improved security of your data and network, which reduces the likelihood of a breach
- Independent validation of vulnerability remediation
- Ability to provide peace of mind for your organization and its stakeholders

The table below summarizes the original findings and the results of the retest.

External Penetration Test

Risk Rating	Total	Remediated	Partially Remediated	Not Remediated
High	5	5	0	0
Medium	5	5	0	0
Low	2	2	0	0
Total	12	12	0	0

Internal Vulnerability Assessment

Risk Rating	Total	Remediated	Partially Remediated	Not Remediated	Not Tested
Critical	21	12	8	1	1*
High	16	8	7	1	0
Medium	65	7	58	0	0
Total	103	27	73	2	1

*Finding #2 from the original assessment delivered in October 2020 was not retested due to Carson City restrictions.

The technical details of the retest results, including a full list of the original findings and remediated/not remediated hosts, 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.

Recommendations:

Due to the impact to the overall organization as uncovered by our testing, appropriate resources should be allocated to ensure that remediation efforts are accomplished in a timely manner. While a comprehensive list of items that should be implemented is beyond the scope of this engagement, some high-level items are important to mention. These recommendations repeated from the October 2020 report as the associated findings have not been fully remediated.

1. **Update all systems that are currently running unsupported operating systems**: Lack of support implies that no new security patches for the product will be released by the vendor. As a result, the unsupported operating systems are likely to contain security vulnerabilities. These systems should either be updated to run a supported operating system or shut down in order to protect the security, availability, and integrity of Carson City's infrastructure and data.

2. **Implement and enforce implementation of change control across all systems**: Misconfiguration and insecure deployment issues were discovered across various systems. The vulnerabilities that arose can be mitigated through the use of change control processes on all systems.

3. **Implement a patch management program:** Operating a consistent patch management program per the guidelines outlined in NIST SP 800-40 is an important component in maintaining good security posture. This will help to limit the attack surface that results from running unpatched internal services.

4. **Change default credentials upon installation.** To reduce the risk of security breaches through default credentials which have been left configured on network devices, it's best to implement a process to change the passwords, and if possible, account names, when new equipment is installed.

5. **Conduct regular vulnerability assessments.** As part of an effective organizational risk management strategy, vulnerability assessments should be conducted on a regular basis. Doing so will allow the organization to determine if the installed security controls are installed properly, operating as intended , and producing the desired outcome. Consult NIST 800-30 for guidelines on operating an effective risk management program.

6. **Recommend remediation scanning be performed.** Based on the number of issues identified we would recommend Carson City IT staff work toward remediating issues working on the most critical items first. Retesting should be performed within 6 months of this report.

Risk Rating Information

The findings are summarized within the body of the report and include the assignment of risk and CVSS score. The risk was determined based on our expertise of the defined risk with subjective consideration of the impact to the organization and is not based solely on CVSS.

Critical Risk - A vulnerability identified as "critical risk" should be viewed as an immediate priority for mitigation and remediation. These findings identify conditions in which exploits readily exist and/or are currently being exploited. If exploited will most likely result in the compromise and/or unauthorized access of a networked system, application, or information system. Significant security breaches and/or costly downtime may result if the vulnerability is not mitigated promptly.

High Risk - A vulnerability identified as "high risk" should be viewed as a top priority for mitigation and immediate attention. These findings identify conditions that could directly result in the compromise or unauthorized access of a network, system, application, or information. Significant security breaches or costly downtime may result if the vulnerability is not addressed within an appropriate time frame.

Medium Risk - A vulnerability identified as "medium risk" should be viewed as an essential priority for mitigation which should be addressed as soon as possible. These findings may identify conditions that, while they do not immediately or directly result in a compromise, do provide a capability or information that could result in a compromise or network disruption in combination with other vulnerabilities.

Low Risk - A vulnerability categorized as "low risk" identifies a condition that does not immediately or directly results in a compromise. However, it may provide information that could be used to gain insight into how to compromise or gain unauthorized access to a network, system, application, or information. While they can be prioritized for mitigation at a lower level, they are still of concern and may lead to more severe security threats.

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, closely mimics the real-world, targeted attacks that organizations face daily. In addition, penetration testing for impact is a goal-based assessment, which creates more than a simple vulnerability inventory instead of providing the true business impact. Instead, 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. However, 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 mimic real-world situations closely, enabling customers to have increased access to industry-recognized expertise 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.