VONAHI SECURITY

Monthly Internal network scan

EXECUTIVE SUMMARY

Infowerks Data Services

November 15, 2025

Copyright

Confidentiality

This document contains organization confidential information of a proprietary and sensitive nature. As such, this document should be afforded the security and handling precautions that a confidential document warrants. This document should have a controlled distribution to relevant parties only and should not be copied without written permission. Vonahi Security treats the contents of a security audit as organization confidential material and will not disclose the contents of this document to anyone without written permission.

Assessment Project Team

Below is a list of contacts that were involved in this engagement. Should you have any questions pertaining to the content of this document or any project and non-project-related items, please feel free to reach out to the necessary project contacts.

Primary Point of Contact	
Name:	Alton Johnson
Title:	Principal Security Consultant
Office:	(844) 866-2732
Email:	support@vpentest.io

Executive Summary

Infowerks Data Services has requested the assistance of Vonahi Security to perform a comprehensive security assessment to assist with evaluating the cyber risks presented within the tested environment(s). The objective of this engagement was to determine if any identified threats could be used to mount an attack against the organization that could lead to the disclosure of sensitive information or access to critical information systems.

Included in this Executive Summary report is a high-level overview of the results that were observed during this assessment. A copy of more specific information pertaining to technical findings and remediation details are documented within the Technical Report.

Engagement Scope of Work

Prior to beginning the assessment, Vonahi Security and Infowerks Data Services agreed to a scope of work to define the specific assessment phases. The table below outlines the engagement scope of work and details entailed within each assessment phase that was conducted as part of this engagement.

Assessment Component	Assessment Phases
Internal Vulnerability Assessment	The internal network environment was scanned for common and documented security vulnerabilities. It should be noted that no vulnerabilities were exploited in this assessment, only identified. → **Vulnerability Assessment** - A vulnerability assessment was also performed against the list of systems provided for the scope for testing. This vulnerability assessment attempted to identify, but not exploit, security vulnerabilities that exist within the environment.

Engagement Statistics

The information below displays overall statistics that were recorded as part of this engagement. Following the statistics, Vonahi Security has summarized all of the threats identified.

Internal Vulnerability Assessment

The information below provides a high-level overview of the assessment results recorded as part of this engagement. Following this section is a summary of all the threats identified and their potential risk to your organization.

Overall Severity Ranking

ASSESSMENT SCHEDULE

Sat, November 15, 2025
12:06 AM PT

Immediate remediation or mitigation is required. Exploitation of identified vulnerabilities require minimal effort from an attacker and pose a significant threat. A successful attack could result in unauthorized access to systems and/or valuable data.

Engagement Results Charts

To help Infowerks Data Services understand the severity of the threats identified during testing, Vonahi Security has included an overall summary chart below that displays a comparison of the report findings as well as the vulnerabilities that were discovered.

Vonahi Security performed a vulnerability assessment to provide additional value and insight as to the vulnerabilities that were identified by our vulnerability scanner. This vulnerability scan included the discovery of common security vulnerabilities that are publicly documented with Common Vulnerabilities and Exposures (CVE) scores.

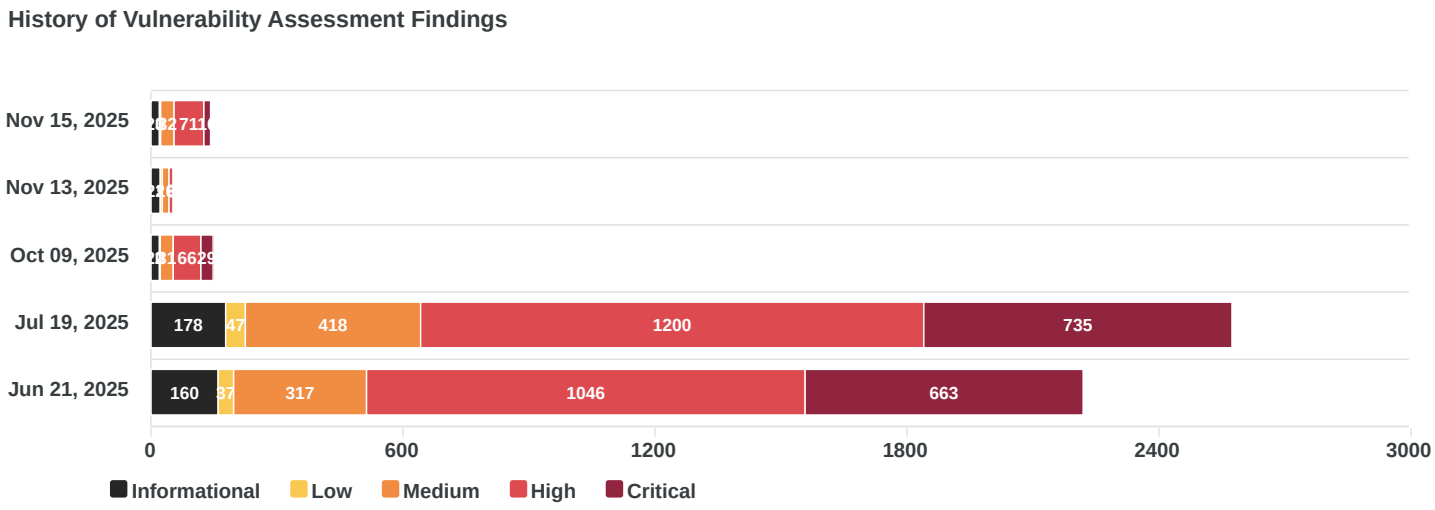
VULNERABILITY ASSESSMENT FINDINGS

142 TOTAL

16 CRITICAL	71 HIGH	32 MEDIUM	3 LOW	20 INFO

Comparison Charts

To help Infowerks Data Services understand the trend of the PenTest Findings and vulnerabilities discovered in the past as part of this on-going engagement, Vonahi Security has provided trend data in this section of the report.



Engagement Results Summary

To summarize the results, Vonahi Security has grouped all of the findings from the penetration test into rollup findings. These rollup findings can be used to quickly determine the root cause of the issues identified in the technical report. By implementing a remediation strategy for the findings based on the rollup issues identified below, Infowerks Data Services's security posture would be greatly improved.

Internal Vulnerability Assessment

Category	Summary
N/A	N/A

Remediation Roadmap

For each assessment conducted, Vonahi Security provided a remediation roadmap to help Infowerks Data Services understand the issues within the respective environment and the overall remediation strategies that should be implemented to resolve the issues identified during the penetration test. It should be noted that the remediation strategies below apply to multiple issues identified within the technical report and can greatly reduce the overall attack surface once successfully implemented.

Internal Vulnerability Assessment

Issue	Remediation Strategy
N/A	N/A