# Roger Insurance Risk Findings

August 19, 2024

Powered by cynomi

# Introduction

The following findings offer an aerial view of the risk landscape as surveyed by the latest scans performed, per source. Undertaking numerous scans of your chosen scan targets while using multiple sources improves the accuracy of your score, broadens your understanding of the threat environment, improves the precision of locating vulnerabilities and deepens insight into your organization's exposure to risk.

This report is based on 11 scanned targets from the following sources: Internal Cynomi scan, Microsoft Secure Score, External Cynomi scan, External Nessus scan, which has culminated in the generation of a risk score.
Your risk score is expressed as a number 0-10, representing the level of safety against threat exposure, with 1 being the lowest score and 10 being the highest.

# Risk score

## Your Score*

Across all industries

4.9 Medium

Within Insurance and Finance

4.1 Medium

* Score derived from 11 scanned targets using 4 sources

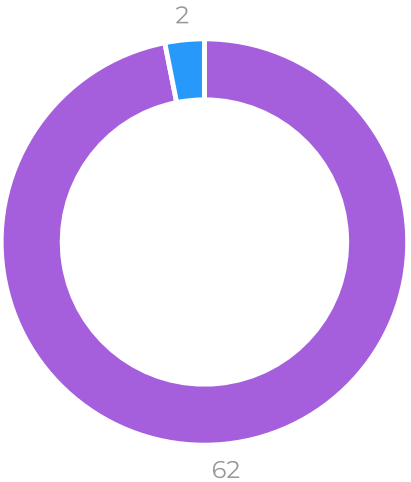
## Severity

64

Findings detected

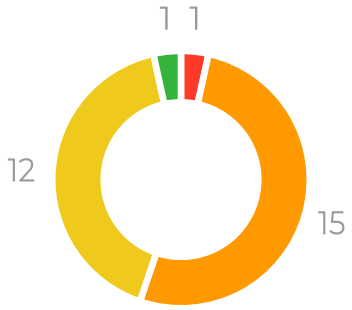
| | |
|---|---|
| 2 Critical | 16 High |
| 42 Medium | 2 Low |
| 2 Info | |

## Findings
## Info vs. To address



# Findings per source

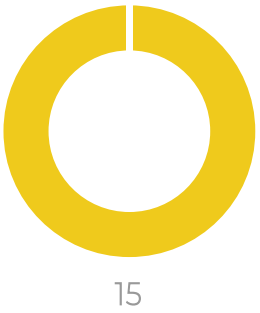
## Internal Cynomi scan




7 targets scanned

Total: 29

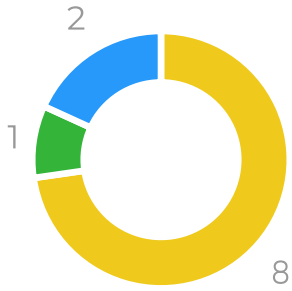
## Microsoft Secure Score




1 targets scanned

Total: 15

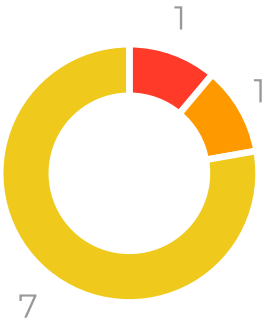
## External Cynomi scan




2 targets scanned

Total: 11

## External Nessus scan




1 targets scanned

Total: 9

# Findings per security domain

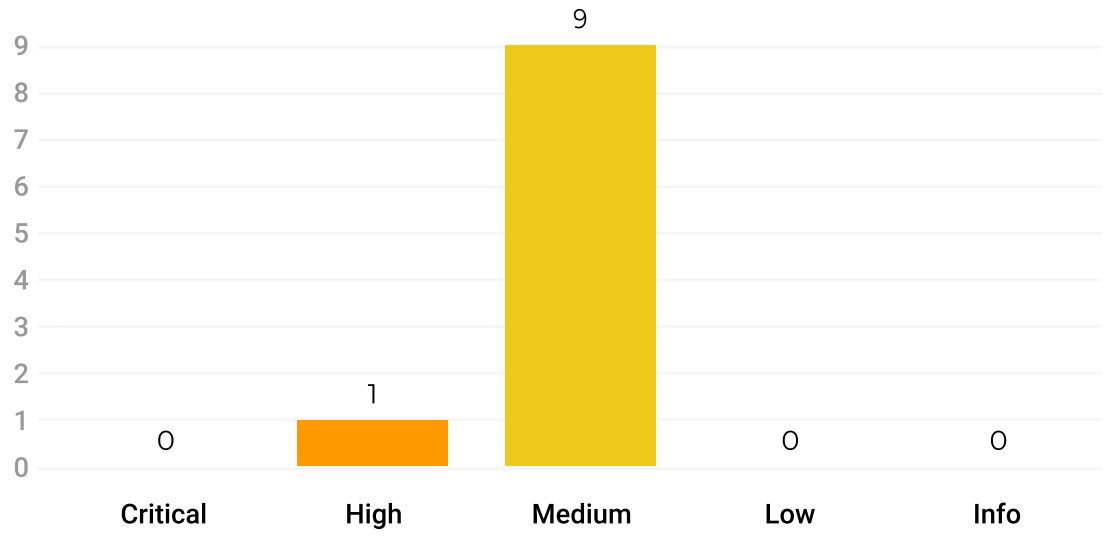
Findings may apply to one or more security domains, or exist independently. The following results relate to findings that correspond with a security domain.

| DOMAIN | CRITICAL | HIGH | MEDIUM | LOW | TO ADDRESS | INFO |
|---|---|---|---|---|---|---|
| Domain and DNS | 0 | 0 | 0 | 1 | 1 | 0 |
| On-Premises Network | 0 | 0 | 0 | 0 | 0 | 2 |
| Website and Web Application | 0 | 0 | 8 | 0 | 8 | 0 |

# Vulnerability

All page results relate to findings containing Common Vulnerabilities and Exposures (CVEs).
A CVE is a glossary that classifies vulnerabilities according to their threat level.

## Vulnerability by severity




## Vulnerability summary

| SEVERITY | SCAN TARGET | CVES | PRODUCTS |
|---|---|---|---|
| Critical | 0 | 0 | 0 |
| High | 1 | 1 | 1 |
| Medium | 2 | 9 | 3 |
| Low | 0 | 0 | 0 |
| Info | 0 | 0 | 0 |

* SCAN TARGET - relates to the number of scanned identifiers (e.g.: IP address)
CVEs - indicates the number of CVEs found
PRODUCTS - refers to the amount of software packages on which vulnerabilities were discovered

# Appendix - scan targets

11 total targets scanned

| SCAN TARGET | SOURCE |
| --- | --- |
| 127.7.4.123 | External Nessus scan |
| 137.74.187.103 | External Cynomi scan |
| 192.16.0.11 | Internal Cynomi scan |
| 192.161.0.11 | Internal Cynomi scan |
| 192.161.0.110 | Internal Cynomi scan |
| 192.161.12.10 | Internal Cynomi scan |
| 192.168.0.10 | Internal Cynomi scan |
| 192.168.0.11 | Internal Cynomi scan |
| 192.168.0.13 | Internal Cynomi scan |
| https://hackthissite.org | External Cynomi scan |
| Microsoft 365 Cloud | Microsoft Secure Score |