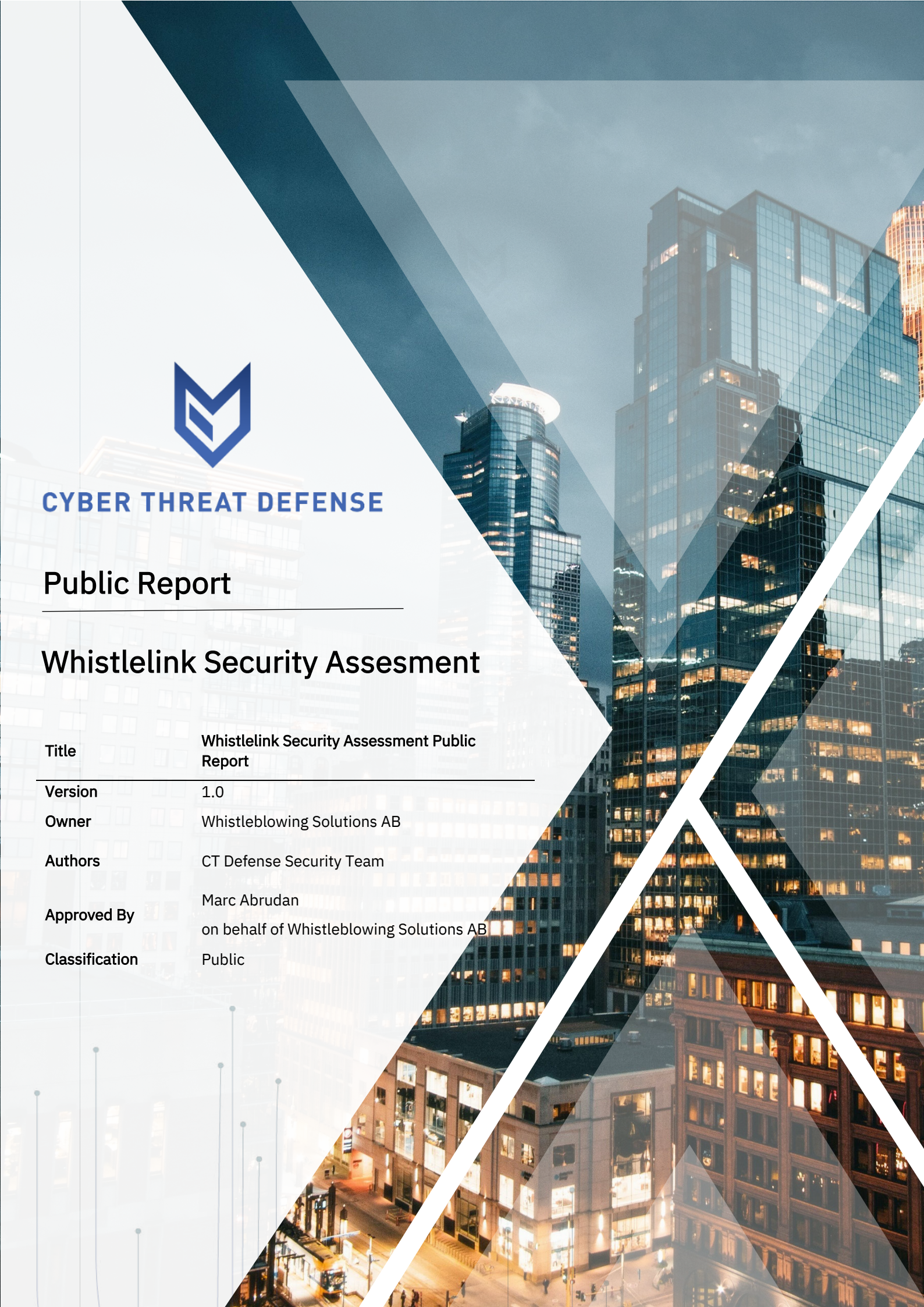


CYBER THREAT DEFENSE

Public Report

Whistlelink Security Assesment

Title	**Whistlelink Security Assessment Public Report**
Version	1.0
Owner	Whistleblowing Solutions AB
Authors	CT Defense Security Team
Approved By	Marc Abrudan on behalf of Whistleblowing Solutions AB
Classification	Public

Document Control

Version	Date	Author	Change Description
0.1	May 24, 2021	Costica Luchian	Security Assessment Start
0.2	May 31, 2021	Costica Luchian	Security Assessment Report Delivery
0.3	July 13, 2021	Costica Luchian	Vulnerability Remediation Verification Completed
1.0	July 16, 2021	Razvan Furdui	Public Report Delivery

CYBER THREAT DEFENSE
TURNING CYBER THREATS INTO ACTIONABLE INSIGHTS

Legal name: CT DEFENSE SRL

Fiscal Code: RO38412840

Phone: 0040 752607204

Email: info@CTDefense.com

Website: CTDefense.com

Independent Security Assessment Report

To Whom It May Concern:

CTDefense LTD ("CTDefense") has performed the Web Application Security Assessment for Whistleblowing Solutions AB, Inc ("Client") while acting as an independent security assessor. This assessment was performed with the intent of evaluating the scope, security, and resiliency of Client's Whistlelink application environments.

The methodology utilized during this assessment is detailed in Methodology. CTDefense developed this methodology based on extensive professional experience and information system security assessment best practices gathered from the Open Source Security Testing Methodology Manual ("OSSTMM"), the National Institute of Standards and Technology ("NIST") Special Publication 800-115: Technical Guide to Information Security Testing and Assessment, the Penetration Testing Execution Standard ("PTES"), and the Open Web Application Security Project ("OWASP") Testing Guide v4.0.

While this type of assessment is intended to mimic a real-world attack scenario, CTDefense is bound by rules-of-engagement, defined scope, allocated time, and additional related constraints. CTDefense has made every effort to perform a thorough and comprehensive analysis and to provide appropriate remedial advice. However, inherit limitations, errors, misrepresentations, and changes to the Client environment may have prevented CTDefense from identifying every security issue that was present in the Client environment at the time of testing. Therefore, the findings included in this report should be considered to be representative of what a similarly skilled attacker could achieve with comparable resources, constraints, and time frame.

Additionally, it is worth emphasizing that the findings and remediation recommendations are the result of a point-in-time assessment based on the state of the Client environment as of May 31, 2021. CTDefense therefore does not provide any assurance related to configuration or control modifications in the Client environment, changes in regulatory or compliance requirements, discoveries of new vulnerabilities and attack techniques, or any other future event that may impact the Client's security posture.

The information contained in this report represents a fair and unbiased assessment of the Client's environment based on the agreed upon criteria as defined in the Statement of Work. This report is provided to the Client as notification of outstanding security risks that threaten the confidentiality, integrity, and availability of sensitive information, as well as to provide assistance and direction with remediation. The evidence and references provided for each finding serve as the basis for our qualified opinions in this report.

CTDefense has provided this report solely for private and internal use by the Client, and it may not be shared or redistributed without CTDefense's express written consent. CTDefense's assessments focus exclusively on information security and the conclusions arrived at in this report should not be considered to be a representation or endorsement of the Client's products of services.

Andrei Pusoiu

Quality Control Manager

CTDefense, LTD

Management Summary

Initial Information

CT Defense performed Web Application Security Assessment to assess the risk that a real-life, targeted attacker poses to the security and integrity of the Whistleblowing Solutions AB Whistlelink. Understanding the current vulnerabilities is the first step in remediating and ultimately enhancing Whistleblowing Solutions AB's overall security maturity.

The purpose of the assignment was to identify any risks or potential issues that could impact the Confidentiality, Integrity, or Availability of the systems in scope.

CT Defense performed testing from both unauthenticated (anonymous) and authenticated perspectives. Unauthenticated testing identifies vulnerabilities and weaknesses available to anyone that possesses network connectivity to the Whistlelink environment. Authenticated testing identifies vulnerabilities and weaknesses in functionality that are only available to valid, authenticated users. Since most applications commonly limit anonymous access and provide the majority of their functionality to authenticated users, authenticated testing often provides the best insight into the security posture of the systems in scope.

Remediation Verification

Remediation verification was performed using an updated system version. All previously identified findings from the initial assessment were validated to confirm if successful remediation had occurred.

Scope of the assessment

The scope of the assessment was limited to the following assets as authorized by the Whistleblowing Solutions AB:

clients-api.preprod.whistlelink.com
clients.preprod.whistlelink.com
[subdomain].preprod.whistlelink.com
admin.preprod.whistlelink.com

Timeframe

The initial Web Application Security Assessment was performed in the dates between May 24, 2021 and May 31, 2021.

Remediation Verification was performed on July 13, 2021.

Limitations

This was a time-boxed security testing engagement. During a time-boxed engagement, the CTDefense team prioritizes testing to assess the most sensitive portions and functions of the application.

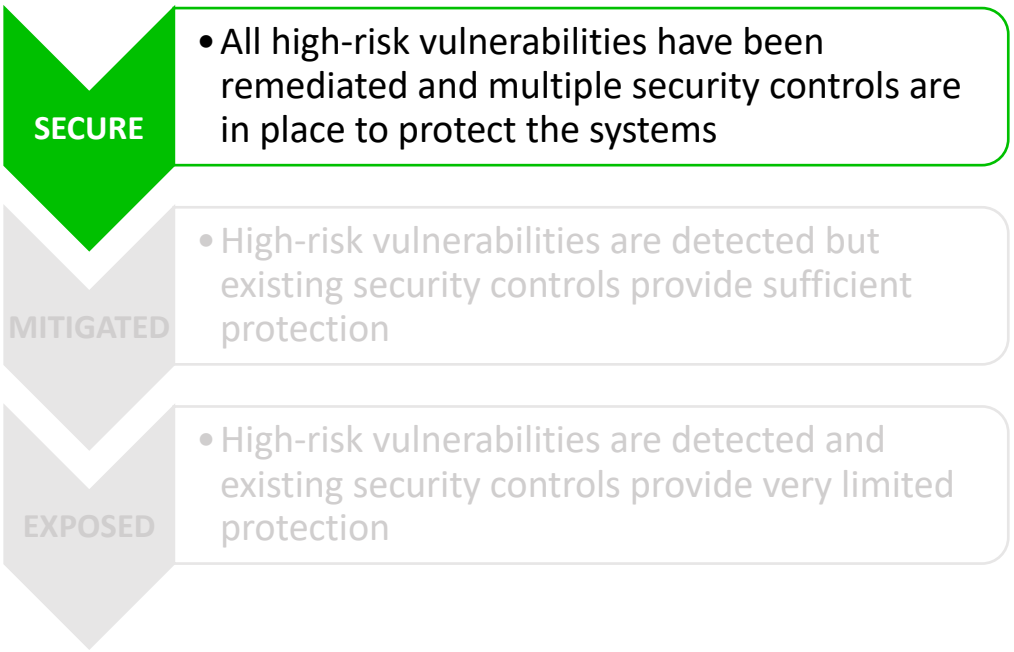
No other specific limitations were defined in the scoping phase by the client.

Summary of Findings

This section documents the results of the Web Application Security Assessment and remediation verification conducted for Whistleblowing Solutions AB. The security assessment was conducted by CT Defense's certified security engineers.

The Security team identified several security vulnerabilities and provided remediation advice to Whistleblowing Solutions AB.

After being notified by Whistleblowing Solutions AB that all vulnerabilities had been remediated, CT Defense performed a remediation test on July 13, 2021 and confirmed that all findings identified were either corrected or had been adequately addressed through other controls.



Identified Security Controls

Security Control in place	State
Authorization controls which were put in place are strong and effective	Good Practice
No possibility of exfiltrating the DB content out of the application	Good Practice
Updates procedures and immediate remediation followed thoroughly	Good Practice
Strong Password Policy for company users	Good Practice
Authentication mechanism is built to the highest standards	Good Practice

Final Statement

As a result of conducting this engagement and remediation verification, CT Defense has determined that cumulatively the vulnerabilities identified pose a Low risk to Whistlelink. While no application or system can be 100% secure, all the security findings were corrected or addressed and it is confirmed that the systems in scope are reasonably well written from a security perspective and the supporting systems are deployed, configured, and implemented securely.