1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a security assessment conducted on the domain **becu.ft.cashedge.com**. The analysis was performed using a Basic scan type, initiated on **04-07** at **18:00** and completed in **00h:10m:39s**. The evaluation focused on identifying High and Medium-risk issues, with a particular emphasis on SSL/TLS configurations and certificate management.

1.2 Summary of Findings

The security assessment identified a total of **18 issues**, categorized as **0 High-risk**, **1 Medium-risk**, **1 Low-risk**, and **16 informational**. The most significant finding is a Medium-risk issue related to SSL certificate expiration, with one domain having **72 days** remaining before renewal is required, indicating a need for timely action to avoid potential service disruptions. Additionally, a Low-risk issue was noted in the SSL/TLS protocols, with TLS 1.2 being the minimum standard used, and no support for the more secure TLS 1.3. The assessment revealed no high-density service configurations or shared hosting risks, and all services are operating on standard ports, minimizing exposure to brute force attacks. These findings suggest a generally secure environment but emphasize the importance of addressing SSL-related vulnerabilities to maintain a robust security posture.

Title	Risk
SSL Certificate Expiration Analysis	Medium
SSL/TLS Protocols Security Assessment	Low

1.3 Detailed Findings

1.3.1 SSL Certificate Expiration Analysis

Description:

The domain **becu.ft.cashedge.com** has an SSL/TLS certificate expiring in **72 days**, categorized under the “Warning” risk level. This indicates that renewal planning should occur soon to prevent potential service disruptions and maintain secure communications.

Affected Assets:

- Domain: **becu.ft.cashedge.com**

Recommendations:

- Initiate the renewal process for the SSL/TLS certificate well before the expiration date to ensure continuous secure service. - Implement automated monitoring tools to alert when certificates are nearing expiration to prevent oversight.

1.3.2 SSL/TLS Protocols Security Assessment

Description:

The analysis revealed that the domain is using TLS 1.2 as the minimum standard, with no support for TLS 1.3. While TLS 1.2 is currently acceptable, adopting TLS 1.3 would enhance security and performance due to its improved cryptographic algorithms and reduced handshake latency.

Affected Assets:

- **1 endpoint** is using TLS 1.2.

Recommendations:

- Upgrade to TLS 1.3 to leverage its advanced security features and performance improvements.
- Regularly review and update cryptographic protocols to align with industry best practices and standards.

1.4 General Recommendations

To maintain a strong security posture, it is recommended to:

- Regularly review and update all SSL/TLS configurations and certificates.
- Implement automated systems for monitoring certificate expirations and protocol compliance.
- Stay informed about emerging security standards and integrate them into your infrastructure promptly.
- Conduct periodic security assessments to identify and mitigate potential vulnerabilities proactively.

By following these recommendations, the organization can ensure robust protection against potential threats and maintain secure operations.