1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **api-csc-stg-sgw-vip.it.hpe.com**. The analysis commenced on **August 2nd** at **23:00** and concluded after a duration of **19 minutes and 31 seconds**. The assessment was identified by tracking ID **02ff2392f2c7** and followed a basic scan type methodology. The primary objective was to identify and evaluate potential security vulnerabilities within the web application and infrastructure, focusing on High and Medium-risk issues.

1.2 Short Summary of Main Issues

The security assessment identified a total of **20 issues**, categorized as **1 High-risk**, **2 Medium-risk**, **3 Low-risk**, and **14 informational**. The most critical finding is a High-risk Denial of Service (DoS) vulnerability, with a **95.34%** timeout rate on port **80**, necessitating immediate action to prevent potential service disruptions. Medium-risk issues include the absence of a Web Application Firewall (WAF) on **100%** of analyzed hosts, increasing susceptibility to injection attacks, and sensitive subdomain naming that could expose critical systems. Immediate remediation efforts should focus on mitigating the DoS vulnerability and enhancing WAF coverage to safeguard against cyber threats.

1.3 Key Security Issues

Title	Risk
Denial of Service (DoS)	High
Absence of WAF	Medium
Subdomain Naming Security	Medium
API Surface Analysis	Low
TCP Wrapped Ports	Low
SSL Certificate Expiration	Low

1.3.1 Denial of Service (DoS)

Description A high-risk Denial of Service (DoS) vulnerability was identified with a significant timeout rate of **95.34%** on port **80**. This indicates a severe risk of service disruption, potentially affecting the availability of the web application.

Affected Assets

- Endpoint: **api-csc-stg-sgw-vip.it.hpe.com:80**

Recommendations Immediate implementation of DoS protection measures is recommended. This includes configuring rate limiting, deploying network-level DoS protection solutions, and ensuring robust monitoring to detect and mitigate potential attacks swiftly.

1.3.2 Absence of WAF

Description The absence of a Web Application Firewall (WAF) was detected on **100%** of the analyzed hosts, resulting in a heightened vulnerability to injection attacks and unauthorized data access.

Affected Assets

- Host: **api-csc-stg-sgw-vip.it.hpe.com**

Recommendations Deploy a Web Application Firewall (WAF) to provide an additional layer of security against common web application attacks such as SQL injection and cross-site scripting (XSS). Regularly update WAF rules to adapt to emerging threats.

1.3.3 Subdomain Naming Security

Description Sensitive subdomain naming was observed, which could potentially expose critical systems such as administrative interfaces or development environments.

Affected Assets

- Subdomain: **api-csc-stg-sgw-vip.it.hpe.com**

Recommendations Review and modify subdomain naming conventions to avoid revealing sensitive information about internal systems. Implement access controls and monitoring for sensitive endpoints to prevent unauthorized access.

1.4 General Recommendations

To enhance the overall security posture, it is crucial to address the identified High and Medium-risk issues promptly. Implementing a comprehensive security strategy that includes regular vulnerability assessments, deploying necessary security controls like WAFs, and maintaining up-to-date security patches will significantly reduce the risk of exploitation. Additionally, continuous monitoring and incident response planning are essential to detect and respond to potential threats effectively.