|  |  |
| --- | --- |
|  | |
|  | |
|  | |
| VAPT Report – Auto Reconciliations  Internet Banking Penetration Testing and Vulnerability Assessment | |
| 31 October 2022 | Document Version 0.02 | |
|  | |
|  |  |

Dimension Data contact details

We welcome any enquiries regarding this document, its content, structure, or scope. Please contact:

Ayub Mwangi - Senior Information Security Engineer, Mobile Phone: 0727517942

Dimension Data Solutions Ltd

Purshottam Place

Westlands Road

Nairobi

0727517942

ayub.mwangi@dimensiondata.com

Please quote reference in any correspondence or order.

Confidentiality

This document contains confidential and proprietary information of Dimension Data Solutions Ltd ('Dimension Data'). Auto Reconciliations may not disclose the confidential information contained herein to any third party without the written consent of Dimension Data, save that Auto Reconciliations may disclose the contents of this document to those of its agents, principals, representatives, consultants or employees who need to know its contents for the purpose of Auto Reconciliations’s evaluation of the document. Auto Reconciliations agrees to inform such persons of the confidential nature of this document and to obtain their agreement to preserve its confidentiality to the same extent as Auto Reconciliations. As a condition of receiving this document, Auto Reconciliations agrees to treat the confidential information contained herein with at least the same level of care as it takes with respect to its own confidential information, but in no event with less than reasonable care. This confidentiality statement shall be binding on the parties for a period of five (5) years from the issue date stated on the front cover unless superseded by confidentiality provisions detailed in a subsequent agreement.

Terms and conditions

This document is valid until 30 November 2022 and, in the absence of any other written agreement between the parties, Dimension Data and Auto Reconciliationsacknowledge and agree is subject to Dimension Data’s standard terms and conditions which are available on request or at [dimensiondata.com/en-gb/legal](https://www.dimensiondata.com/en-gb/legal) . Dimension Data reserves the right to vary the terms of this document in response to changes to the specifications or information made available by Faulu. Submission of this document by Dimension Data in no way conveys any right, title, interest, or license in any intellectual property rights (including but not limited to patents, copyrights, trade secrets or trademarks) contained herein. All rights are reserved.

Dimension Data does not assume liability for any errors or omissions in the content of this document or any referenced or associated third party document, including, but not limited to, typographical errors, inaccuracies, or out-dated information. This document and all information within it are provided on an 'as is' basis without any warranties of any kind, express or implied. Any communication required or permitted in terms of this document shall be valid and effective only if submitted in writing.

All contracts with Dimension Data will be governed by Kenyan Law and be subject to the exclusive jurisdiction of the Kenyan courts.

Document configuration management

Document identification

|  |  |
| --- | --- |
| Title | Internet Banking Penetration Testing and Vulnerability Assessment |
| Document Type | VAPT Report |
| File Name | output.docx |
| Version | Version 0.01 |
| Sensitivity Classification | Company Confidential - Client / Vendor Information |
| Document Owner | Ayub Mwangi |

Preparation

| Action | Name | Role / Function | Date |
| --- | --- | --- | --- |
| Prepared by: | Rashpal Mediratta | Information Security Engineer | 2022-11-28 |
| Reviewed/Approved by: | Ayub Mwangi | Senior Information Security Engineer | 2022-11-28 |

Release

|  | Date Released | Change Notice | Remarks |
| --- | --- | --- | --- |
| 0.01 | 2022-06-17 | Release | 1st Draft |

Contribution (C) and distribution (D) list

| Name | C/D | Organisation | Title |
| --- | --- | --- | --- |
| Rashpal Mediratta | C | Dimension Data | Information Security Engineer |
| Ayub Mwangi | C & D | Dimension Data | Senior Information Security Engineer |

Table of Contents

[1. About This Design Document 5](#_Toc115681491)

[1.1. Document Purpose 5](#_Toc115681492)

[1.2. Intended Audience 5](#_Toc115681493)

[1.3. Document Usage Guidelines 5](#_Toc115681494)

[2. Executive Summary 6](#_Toc115681495)

[2.1. Introduction 6](#_Toc115681496)

[2.2. Scope 6](#_Toc115681497)

[2.3. Risk Rating Matrix 7](#_Toc115681498)

[2.4. Vulnerability Assessment Review 8](#_Toc115681499)

[Appendix A VA Report acceptance 14](#_Toc115681500)

List of Figures

[Figure 1: Vulnerability Distribution 9](#_Toc106372946)

List of Tables

[Table 2: Risk Rating Matrix 7](#_Toc115681501)

[Table 3: Vulnerability Count Per Host 8](#_Toc115681502)

[Table 4: Summary of Key Findings 10](#_Toc115681503)

[Table 5: Security Headers 12](#_Toc115681504)

# About This Design Document

## Document Purpose

The purpose of this document is to provide in detail the recommended findings and remediations for the network. This document provides details on the findings and remediations that can be implemented to have a better overall security posture.

## Intended Audience

The intended audience of this document are Fauli Microfiance / Dimension Data technical staff who will be implementing and operating the new network.

## Document Usage Guidelines

The document should be used as a guideline for deriving the necessary information to ultimately remediate the findings that were discovered during the external assessment.

* This document comprises the following components: -
* In Scope URL’s
* Findings
* Remediations
* Vulnerability References
* Evidence

# Executive Summary

## Introduction

We have the pleasure of presenting the main findings on our VA scan of as enumerated and documented in the shared IPs. We also want to express our appreciation to for the support given by the respective staff during this review.

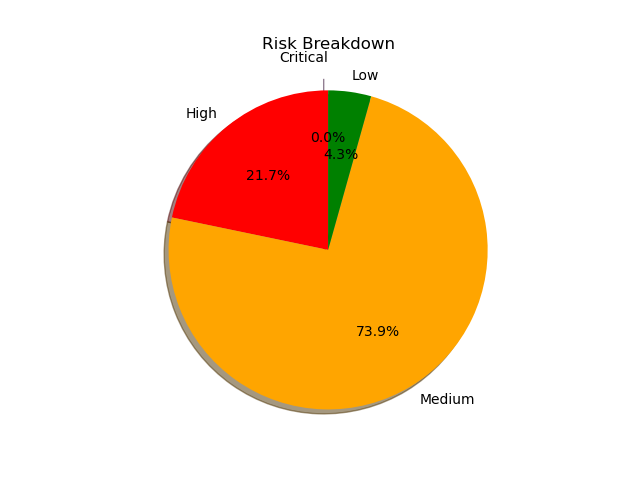
## Scope

The following IP addresses were in scope for the vulnerability Assessment:

|  |  |
| --- | --- |
| IPs | IPs 10.1.15.60,10.1.15.52,10.1.15.53,172.16.4.67,172.16.4.65 |

## **Risk Break down**

The breakdown of the vulnerabilities is as follows: Critical Vulnerabilities account for 0% of the total vulnerabilities, High severity vulnerabilities account for 21.74% of the total vulnerabilities, Medium severity vulnerabilities account for 73.91% of the total vulnerabilities, Low severity vulnerabilities account for 4.35% of the total vulnerabilities. Highest risk is Medium



## **Host Breakdown**

The host with the highest risk is 172.16.4.65 with 12 vulnerabilities,which accounts for 52.17% of the total vulnerabilities.The Top 5 hosts with the most vulnerabilities are: ['172.16.4.65', '172.16.4.67', '10.1.15.52'] with [12, 6, 5] vulnerabilities which accounts for 100.0% of the total vulnerabilities respectively.

## **Common Vulnerabilities**

The most common vulnerability is TLS Version 1.0 Protocol Detection with 4 occurences and a risk of Medium. Its solution is to Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.The second most common vulnerability is TLS Version 1.1 Protocol Deprecated with 4 occurences and a risk of Medium. Its solution is to Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.The third most common vulnerability is SSL Medium Strength Cipher Suites Supported (SWEET32) with 3 occurences

## **Critical Vulnerabilities**

The most common vulnerability is SSL Medium Strength Cipher Suites Supported (SWEET32) with 3 occurencesand a risk of High. Its solution is to Reconfigure the affected application if possible to avoid use of  
medium strength ciphers.The Second most common vulnerability is SSL Certificate Signed Using Weak Hashing Algorithm with 1 occurencesand a risk of High. Its solution is to Contact the Certificate Authority to have the SSL certificate reissued.The Third most common vulnerability is Apache Tomcat 10.0.0.M1 10.0.27 vulnerability with 1 occurences and a risk of High. Its solution is to Upgrade to Apache Tomcat version 10.0.27 or later.

## Risk Rating Matrix

Risks are classified as Critical, High, Moderate or Low as per the matrix defined below.

| Rating | Description |
| --- | --- |
| Critical | Loss of [confidentiality | integrity | availability] is proven and is currently being exploited in the wild.  Countermeasures recommended to mitigate these risks should be implemented as soon as possible and the environment should be reviewed for any signs of  compromise. |
| High | Loss of [confidentiality | integrity | availability] is likely to have a serious adverse effect on the organization or individuals associated with the organization (e.g.,  employees, customers).  Countermeasures recommended to mitigate these risks should be implemented as soon as possible |
| Medium | Loss of [confidentiality | integrity | availability] is likely to have a moderately adverse effect on the organization or individuals associated with the organization (e.g.,  employees, customers).  Countermeasure implementation should be planned for the near future |
| Low | Loss of [confidentiality | integrity | availability] is likely to have only a limited to little adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).  Countermeasure implementation will enhance security and  is of less urgency than the above risks. |

Table 1: Risk Rating Matrix

## Vulnerability Assessment Review

### Vulnerability Assessment Summary Findings

This section details the summary findings of the vulnerability Assessment conducted on the IPs in scope.

**NB: The detailed findings have been shared as an addendum to this report. It serves as the remediation tracker**

### Vulnerability Count

| IP Address | Critical | High | Medium | Low |
| --- | --- | --- | --- | --- |
| 10.1.15.52 | 0 | 1 | 3 | 1 |
| 10.1.15.53 | 0 | 0 | 0 | 0 |
| 10.1.15.60 | 0 | 0 | 0 | 0 |
| 172.16.4.65 | 0 | 3 | 9 | 0 |
| 172.16.4.67 | 0 | 1 | 5 | 0 |
| Total | 0 | 0 | 0 | 0 |

Table 2: Vulnerability Count Per Host

### Summary of Key Findings

This section defines the Vulnerabilities found as well as their risks.

| Vulnerability | Count | Severity |
| --- | --- | --- |
| SSL/TLS Diffie-Hellman Modulus = 1024 Bits (Logjam) | 1 | Low |
| Apache Tomcat Default Files | 1 | Medium |
| SMB Signing not required | 2 | Medium |
| SSL Self-Signed Certificate | 3 | Medium |
| SSL Certificate Cannot Be Trusted | 3 | Medium |
| TLS Version 1.1 Protocol Deprecated | 4 | Medium |
| TLS Version 1.0 Protocol Detection | 4 | Medium |
| SSL Certificate Signed Using Weak Hashing Algorithm | 1 | High |
| Apache Tomcat 10.0.0.M1 10.0.27 vulnerability | 1 | High |
| SSL Medium Strength Cipher Suites Supported (SWEET32) | 3 | High |

Table 3: Summary of Key Findings

### Prioritizations

This section indicates which vulnerabilities on which asset poses the greatest risk to Auto Reconciliations We recommend that they are addressed first to address the highest risks.

|  |  |  |
| --- | --- | --- |
| **Vulnerability Title** | **SSL Medium Strength Cipher Suites Supported (SWEET32)** | |
| Risk Profile | CVSS3 Score | 5.0 |
| Risk Factor | Medium |
| Exploitability | Ease |  |
| Exploit Available | Exploited by malware: |
| IP | 172.16.4.65 172.16.4.67 | |
| Synopsis | The remote service supports the use of medium strength SSL ciphers. | |
| Solution | Reconfigure the affected application if possible to avoid use of medium strength ciphers. | |
| Reference | CVE | CVE-2016-2183 |
| Links | https://www.openssl.org/blog/blog/2016/08/24/sweet32/ https://sweet32.info |
| **Vulnerability Title** | **SSL Certificate Signed Using Weak Hashing Algorithm** | |
| Risk Profile | CVSS3 Score | 5.0 |
| Risk Factor | Medium |
| Exploitability | Ease | Exploits are available |
| Exploit Available | true  Exploited by malware: |
| IP | 172.16.4.65 | |
| Synopsis | An SSL certificate in the certificate chain has been signed using a weak hash algorithm. | |
| Solution | Contact the Certificate Authority to have the SSL certificate reissued. | |
| Reference | CVE | CVE-2004-2761 |
| Links | https://tools.ietf.org/html/rfc3279 http://www.nessus.org/u?9bb87bf2 http://www.nessus.org/u?e120eea1 http://www.nessus.org/u?5d894816 http://www.nessus.org/u?51db68aa http://www.nessus.org/u?9dc7bfba |
| **Vulnerability Title** | **SSL/TLS Diffie-Hellman Modulus = 1024 Bits (Logjam)** | |
| Risk Profile | CVSS3 Score | 2.6 |
| Risk Factor | Low |
| Exploitability | Ease | No known exploits are available |
| Exploit Available | Exploited by malware: |
| IP | 10.1.15.52 | |
| Synopsis | The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. | |
| Solution | Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater. | |
| Reference | CVE | manual |
| Links | https://weakdh.org/ |
| **Vulnerability Title** | **Apache Tomcat 10.0.0.M1 10.0.27 vulnerability** | |
| Risk Profile | CVSS3 Score | 7.8 |
| Risk Factor | High |
| Exploitability | Ease | No known exploits are available |
| Exploit Available | Exploited by malware: |
| IP | 10.1.15.52 | |
| Synopsis | The remote Apache Tomcat server is affected by a vulnerability | |
| Solution | Upgrade to Apache Tomcat version 10.0.27 or later. | |
| Reference | CVE | CVE-2022-42252 |
| Links | http://www.nessus.org/u?8445ee2a http://www.nessus.org/u?2a59e27c |

Table 4: Prioritizations

### Strategic Recommendations

To continuously map out and manage the attack surface, have a patch management process in place to:

* + - 1. Remove unused dependencies, unnecessary features, components, files, and documentation.
      2. Continuously inventory the versions of both client-side and server-side components (e.g., frameworks, libraries) and their dependencies
      3. Monitor for libraries and components that are unmaintained or do not create security patches for older versions. If patching is not possible, consider deploying a virtual patch to monitor, detect, or protect against the discovered issue.
      4. A penetration test should be done when considerable change has been introduced to the system.

1. VAPT Report acceptance

I hereby confirm acceptance and agreement of VAPT Report document for the Internet Banking Penetration Testing and Vulnerability Assessment for and the contents contained within, excluding the exceptions described in the notes below.

Notes:

|  |  |  |
| --- | --- | --- |
|  | | |
|  | | |
|  | | |
|  | | |
|  | | |
|  | | |
|  | | |
| Dimension Data |  |  |
|  |  |  |
| Signature |  | Signature |
|  |  |  |
| Print Name and Title |  | Print Name and Title |
|  |  |  |
| Date |  | Date |

should send this signed VAPT Report Acceptance Sheet to ayub.mwangi@dimensiondata.com