**Vulnerability Assessment and Penetration Testing Report**

**For**

**Router**

|  |  |
| --- | --- |
|  | **Cashgro Digital Platform Pvt Ltd** |
| **607, 6th Floor, DLF City Court, Sikanderpur, Nathupur, Sector 24, Gurugram, Haryana 122002** |

|  |  |
| --- | --- |
| **Report Release Date** | 23-July-2024 |
| **Type of Audit** | Security Assessment |
| **Type of Audit Report** | First Audit Report |
| **Period** | 19-July-2024 to 22-July-2024 |

**ITOrizin Technology Solutions Pvt. Ltd.**

An ISO 9001:2015, 20000-1:2011 and 27001:2013 Certified Company

8/14, Sahid Nagar, Gnd. Floor, Kolkata 700078

Ph: +91 33 2415 6011

E-Mail: [connect@itorizin.in](mailto:connect@itorizin.in)

[www.itorizin.com](http://www.itorizin.com/)

**Document Control**

|  |  |
| --- | --- |
| **Document Preparation** | |
| **Document Title** | Security Assessment Report of Internal IP for Cashgro |
| **Document ID** | ITOTSPL-CASHGRO-EVAPT-2024-01-1 |
| **Document Version** | 1.0 |
| **Prepared by** | Subhabrata Chakraborty |
| **Reviewed by** | Susanta Saha |
| **Approved by** | Debjyoti Chowdhury |
| **Released by** | Subhabrata Chakraborty |
| **Release date** | 23-July-2024 |

|  |  |  |
| --- | --- | --- |
| **Document Change History** | | |
| **Version** | **Date** | **Remarks / Reason of change** |
| 1.0 | 23-July-2024 | First Audit Report |

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Distribution List** | | | |
| **Name** | **Organization** | **Designation** | **Email Id** |
| Kunal Kalra | Cashgro Digital Platform Pvt Ltd | Sr Manager | kunal.kalra@cashgro.in |
| Anindya Kanti Ghosh | ITOrizin | Senior Vice President - Projects | gd.anindya@itorizin.in |
| Debjyoti Chowdhury | ITOrizin | Associate Manager - GRC | c.debjyoti@itorizin.in |
| Susanta Saha | ITOrizin | Sr. Security Analyst | s.susanta@itorizin.in |
| Sirsendu Bharati | ITOrizin | Associate Manager - GRC | b.sirsendu@itorizin.in |
| Subhabrata Chakraborty | ITOrizin | Security Analyst | c.subhabrata@itorizin.in |

Contents

[**Introduction** 4](#_Toc172562835)

[**Engagement Scope** 5](#_Toc172562836)

[**Details of the Auditing team** 6](#_Toc172562837)

[**Audit Activities and Timelines** 7](#_Toc172562838)

[**Audit Methodology and Criteria / Standard referred for audit** 8](#_Toc172562839)

[**Tools/ Software used** 9](#_Toc172562840)

[**Executive Summary** 10](#_Toc172562841)

[**Detailed Observations** 11](#_Toc172562842)

[**Appendices** 14](#_Toc172562843)

# **Introduction**

This report presents the results and findings of the Vulnerability Analysis and Penetration Testing conducted on “Internal IP” of “Cashgro” for the Security Assessment program. This assessment was performed by “ITOrizin Technology Solutions Pvt. Ltd.”. The purpose of this assessment was to identify vulnerabilities and other security issues that could affect the “Cashgro’s internal IP”. The findings in this report reflect the conditions found during the testing, and do not necessarily reflect current conditions.

# **Engagement Scope**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S.**  **No** | **Asset**  **Description** | **Criticality**  **of Asset** | **Internal**  **IP Address** | **URL** | **Public**  **IP Address** | **Location** | **Hash Value**  **(in case of applications)** | **Version (in**  **case of applications)** | **Other**  **details such as make and model**  **in case of network devices or security devices.** |
|  | Router | NA | NA | NA | 192.168.1.1 | NA | NA | NA |  |

Date up to which the list has been updated: 22-July-2024

# **Details of the Auditing team**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| S. No | Name | Designation | Email Id | Professional  Qualifications/ Certifications | Whether the resource has Been listed in  the Snapshot information published on CERT-In’s website (Yes/No) |
| 1 | Subhabrata Chakraborty | Jr. Security Analyst | c.subhabrata@itorizin.in | B Tech (CSE) | No |
| 2 | Susanta Saha | Sr. Security Analyst | s.susanta@itorizin.in | B Tech (IT) | Yes |
| 3 | Debjyoti Chowdhury | Associate Manager - GRC | c.debjyoti@itorizin.in | MCA | Yes |
| 4 | Sirsendu Bharati | Sr. Security Analyst | b.sirsendu@itorizin.in | B Tech (IT)  CHFI | Yes |

# **Audit Activities and Timelines**

|  |  |  |  |
| --- | --- | --- | --- |
| Sl. No. | Activities | Start Date | End Date |
|  | Inventory Received | 19-July-2024 | 19-July-2024 |
|  | Automated Scan | 19-July-2024 | 19-July-2024 |
|  | Manual testing | 22-July-2024 | 22-July-2024 |
|  | Report Preparation | 22-July-2024 | 23-July-2024 |
|  | Report Review | 23-July-2024 | 23-July-2024 |
|  | Report Submission | 23-July-2024 | 23-July-2024 |

# **Audit Methodology and Criteria / Standard referred for audit**

The Vulnerability Analysis and Penetration Testing is a form of security testing used to analyze security from inside of a network. The Vulnerability Analysis and Penetration Testing concentrates on client-side safety, file system, hardware, and network security. Cashgro keeps its Security Testing methodology updated with new tools, processes, techniques, or as trend develops. Our methodology is a comprehensive blend of the following methodologies and IT Security industry best practices:

* Open-Source Security Testing Methodology Manual (OSSTMM) from the Institute for Security and Open Methodologies (ISECOM);
* NIST SP 800-115 Technical Guide to Information Security Testing and Assessment.
* Manual Script

# **Tools/ Software used**

|  |  |  |  |
| --- | --- | --- | --- |
| Sl. No | Name of Tool/Software  used | Version of the tool  /Software used | Open Source/Licensed |
|  | Nmap | 7.95 | Open Source |
|  | Kali Linux | 2024.1 | Open Source |
|  | Nessus professional | 10.7.3 | Licensed |
|  | Custom exploits, public exploits | NA | Open Source |

# **Executive Summary**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| S. No | Affected Asset i.e. IP/URL/Application etc | Observation/ Vulnerability title | CVE/CWE | Control Objective # | Control Name # | Audit Requirement # | Severity | Recommendation | Reference | New or  Repeat observation |
|  | 192.168.1.1 | Open ports | NA | NA | NA | NA | Informational | It is recommended to disable all the unwanted ports and services that are not required. | NA | New |

# **Detailed Observations**

|  |  |  |
| --- | --- | --- |
| **Affected Asset:**  **192.168.1.1** | |  |
| **Open ports** | Severity: **Informational** |
| **Service Enumeration:**  **Port Scan Results**   |  |  | | --- | --- | | **IP Address** | **Ports Open** | | **192.168.1.1** | **TCP: 80,443,**  **UDP:** 53 |   **Below are the open tcp ports:** | |

|  |  |
| --- | --- |
| **UPD port scanning result:**    Figure 1: False positive result |  |
| **Vulnerable Points:**  NA |
| **Recommendation:**  It is recommended to disable all the unwanted ports and services that are not required. |
| **Reference:**  NA |
| **New or Repeat observation:** New |

# **Appendices**

**Risk Ranking Approach**

Each assessment finding is assigned a risk rating. The risk rating used in this report is based on the following criteria:

**High**

**Medium**

**Low**

**Info**

Under specific conditions, these vulnerabilities can potentially make the system unusable and lead to serious security breaches. These vulnerabilities violate basic security design parameters and should be handled with the highest priority.

Though the threat is not critical at the moment, it has the potential to become a High risk threat in the future under certain circumstances if not mitigated. Medium risk vulnerabilities require significant mitigation to lower the impact of the threat.

The information found is useful to the attacker, but is not a threat in itself. Existing security controls are likely to be adequate or the risk is acceptable, but over the period this may give rise to more serious problems.

The data revealed is an additional piece of information and there are no serious security implications related to it.

The likelihood of an attack occurring and the impact of a successful attack are used in calculating the risk rating:

Medium

High

Low

Medium

High

Low

**Likelihood**

**Impact**

**Observation Summary**

The overall analytical report is based on the technologies and known threats as of date of penetration testing.

As a result of the audit, the current security posture of the Internal IP within the scope requires security fixes or configurations. During our Internal IP Security Assessment total one (1) observations of Informational category was found. We recommend Cashgro team to implement the recommendations mentioned against the security issues in this report with respect to the affected Internal IP.

**Acronyms:**

* CVE- common vulnerabilities and exposures
* CWE- common weakness enumeration
* MASVS-Firewall Security Verification Standard)
* OWASP- Open Web Application Security Project
* OSSTMM- Open-Source Security Testing Methodology Manual
* ISECOM- ISECOM
* NIST- National Institute of Standards and Technology
* VA-Vulnerability Assessment
* PT-Penetration Testing

**Disclaimer**

The data contained in this document shall not be disclosed, duplicated, used, or disclosed in whole or in part for any purpose. If a contract is awarded because of or in connection with the submission of this data, the client or prospective client shall have the right to duplicate, use, or disclose this data to the extent provided in the contract. This restriction does not limit the client’s or prospective client’s right to use the information contained in the data if it is obtained from another source without restriction.

Although the author or ITOrizin Technology Solutions Pvt. Ltd. have made every effort to ensure that the information in this book was correct at the time of writing, the author and ITOrizin Technology Solutions Pvt. Ltd. do not assume and hereby disclaim any liability to any party for any loss, damage, or disruption caused by errors or omissions, whether such errors or omissions result from negligence, accident, or any other cause.