

**Penetration Testing Report**

For

**EXTERNAL IPS**

At

|  |  |
| --- | --- |
|  | **Cogenthub** |
| **21, Strand Road, Kolkata - 700 001, West Bengal (India)** |

**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/)

**Statement of Confidentiality**

This document contains information that is proprietary and Confidential to “**Cogenthub**” & “**ITOrizin Technology Solutions Pvt Ltd**”, which shall not be disclosed outside to “Cogenthub” and “ITOrizin Technology Solutions Pvt Ltd”, transmitted, or duplicated, used in whole or in part for any purpose other than its intended purpose. Any use or disclosure in whole or in part of this information without explicit written permission of “Cogenthub.” and “ITOrizin Technology Solutions Pvt Ltd” is prohibited.

***“ALL FINDINGS IN THIS REPORT ARE BASED ON THE INFORMATION SHARED WITH “*Cogenthub*” TEAM DURING ASSESSMENT DURATION MENTIONED IN THE ASSESSMENT INFORMATION. ANY CHANGES IN THE SYSTEMS IN SCOPE POST ASSESSMENT DATES MAY NOT REFLECT IN THIS REPORT AND ITORIZIN TEAM IS NOT RESPONSIBLE FOR SUCH ALTERNATIONS”***

**Assessment Information**

|  |  |
| --- | --- |
| Project | External IPs Penetration Testing Report for Cogenthub |
| Prepared by | Subhabrata Chakraborty |
| Classification | Confidential |
| Reviewed By | Susanta Saha |
| Approved By | Debjyoti Chowdhury |
| Assessment Period | 27-Oct-2023 to 02-Nov-2023 |
| Report Date | 02-Nov-2023 |

**Version**

|  |  |  |
| --- | --- | --- |
| Version | Date | Author and Comments |
| 1.0 | 02-Nov-2023 | External IPs Penetration Testing Report for Cogenthub |
|  |  |  |

Contents

[**1** **EXECUTIVE SUMMARY** 4](#_Toc149743704)

[BACKGROUND 4](#_Toc149743705)

[PROJECT TEAM 4](#_Toc149743706)

[**2** **ASSESSMENT METHODOLOGY** 4](#_Toc149743707)

[METHODOLOGY OVERVIEW 4](#_Toc149743708)

[TOOLS USED 4](#_Toc149743709)

[**3** **RISK RANKING APPROACH** 5](#_Toc149743710)

[**4** **SCOPE OF SECURITY ASSESSMENT** 6](#_Toc149743711)

[**5** **SUMMARY OF SECURITY ASSESSMENT FINDINGS** 6](#_Toc149743712)

[**SUMMARY ASSESSMENT RESULT:** 6](#_Toc149743713)

[SUMMARY: TOTAL VULNERABILITY COUNT 6](#_Toc149743714)

[VULNERABILITY SUMMARY 7](#_Toc149743715)

[**6** **SECURITY FINDINGS AND ASSESSMENT DETAILS** 7](#_Toc149743716)

[6.1 DETAILED LIST: FINDINGS & RECOMMENDATIONS 7](#_Toc149743717)

[**7** **ASSESSMENT CONCLUSION** 8](#_Toc149743718)

# EXECUTIVE SUMMARY

This report presents the results and findings of the External IPs Penetration Testing conducted for “Cogenthub” identified as the Penetration Testing 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 External Infrastructure of “Cogenthub”. The security assessment was carried out from the “ITOrizin” premises in Kolkata. The findings in this report reflect the conditions found during the testing, and do not necessarily reflect current conditions.

## BACKGROUND

As part of secure solution and delivery model, “Cogenthub” wanted to identify security weaknesses or vulnerabilities affecting the Public IPs of “Cogenthub”. The security assessment was carried out as per the proposed methodology and also as briefly stated in section 2 of this report.

This report will provide “Cogenthub” the findings and observations from the Public IPs Security Assessment along with the recommendations to fix the vulnerabilities.

## PROJECT TEAM

The assignment was restricted to the contributions of following team members:

|  |  |
| --- | --- |
| **ITOrizin Team** | **Contact details** |
| Debjyoti Chowdhury | Email id: c.debjyoti@itorizin.in |
| Susanta Saha | Email id: s.susanta@itorizin.in |
| Subhabrata Chakraborty | Email id: c.subhabrata@itorizin.in |
| **Cogenthub Team** | **Contact details** |
| NA | Email ID: |

# ASSESSMENT METHODOLOGY

## METHODOLOGY OVERVIEW

Penetration Testing is a repeatable and documented security assessment methodology. A methodology that is kept up-to-date according to changes in the threat environment and industry best practices provides consistency and structure to security testing. ITOrizin Technology Solutions Pvt. Ltd. keeps its Penetration 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.

## TOOLS USED

Typical tools that were used in the security assessment:

* Nmap
* Custom Scripts
* Kali Linux

# 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 now, 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. 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**

# SCOPE OF SECURITY ASSESSMENT

Following Public IPs of Cogenthub were tested during the Penetration Testing:

|  |  |  |
| --- | --- | --- |
| Office Location | Tata IP Address(Primary) | Backup IP Address |
| Martin Burn | 14.99.26.202 | 103.120.188.99 |
| Webel Tower 1 | 14.97.182.234 | 103.121.157.82 |
| Webel Tower 2 | 14.194.112.250 | 202.191.161.121 |
| Gurugram | 49.249.144.186 | 103.101.102.171 |

# SUMMARY OF SECURITY ASSESSMENT FINDINGS

The below sections list the count of total number of vulnerabilities found that are perceived as “High”, “Medium”, “Low” risks and also those which are informational in nature. The security assessment findings are also summarized in the below section.

# **SUMMARY ASSESSMENT RESULT:**

## SUMMARY: TOTAL VULNERABILITY COUNT

During the assessment, no High/ Medium/ Low risk vulnerability has been observed. Only **One (1)** observation was discovered during the assessment.

## VULNERABILITY SUMMARY

The vulnerability findings have been summarized below along with their respective severity rating:

| **Sl. No.** | **Finding** | **CVE:/CWE No.** | **Remediation** | **Vulnerable Points** | **Severity** |
| --- | --- | --- | --- | --- | --- |
|  | Apache test page | N/A | If not required it is advisable to remove the apache test page. | 14.99.26.202 | Informational |

# SECURITY FINDINGS AND ASSESSMENT DETAILS

## 6.1 DETAILED LIST: FINDINGS & RECOMMENDATIONS

|  |  |  |
| --- | --- | --- |
| **Apache test page** | **Informational** |  |
| **Description:**  The Apache HTTP Server version 2.4.18 is operational and accessible via port 80. The "Hello" page likely represents the default landing page provided by Apache when no specific content or configurations have been applied. | |
| **Proof of concept:** | |
| **Vulnerable IPS:**  14.99.26.202:80 | |
| **Remediation:**  If not required it is advisable to remove the apache test page or disable port 80. | |

# ASSESSMENT CONCLUSION

The overall analytical report is based on the technologies and known threats as of date of pen testing. We suggest that all recommendations mentioned in this Public IPs Security Assessment Report should be undertaken in order to ensure the overall security of the concerned Public IPs.

As a result of the assessment, we have found that the current security posture of the Public IPs within the scope have no exploitable vulnerability although we have found out that these public IPs which are configured at firewalls are using the default HTTPS port for login interfaces of those firewalls. We suggest the “Cogenthub” team to host those firewalls in customized HTTPS ports so that no one from outside can access those login interfaces easily.

**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.