**Vulnerability Assessment Report**

**For**



**SAC\_Revisit\_Public**

**March 18, 2022**

**Document Security Level:** Confidential

**Document Version:** 1.0

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Edit Report** | **Editor** |
| 1.0 | March 18, 2022 | Creation | INET Managed Services |

|  |  |  |  |
| --- | --- | --- | --- |
| SAC\_Revisit\_Public | | INET Managed Services CO., LTD. | |
| Name |  | **Name** |  |
| Position |  | **Position** |  |
| Tel |  | **Tel** |  |
| Signature |  | **Signature** |  |

**Table of Contents**

[1. Restrictions on disclosure and use of information 4](#_Toc98507702)

[2. Operation Method 5](#_Toc98507703)

[3. Project Scope 6](#_Toc98507704)

[3.1 Infrastructure Vulnerability Assessment 6](#_Toc98507705)

[4. Testing Tools 7](#_Toc98507706)

[5. Infrastructure Vulnerability Assessment 7](#_Toc98507707)

[5.1 Target Information 8](#_Toc98507708)

[5.2 Executive summary 9](#_Toc98507709)

[5.2.1 Summary Vulnerability by Severity 9](#_Toc98507710)

[5.2.2 Vulnerability by Target 9](#_Toc98507711)

[5.3 Infrastructure Vulnerability Detail 10](#_Toc98507712)

[6. Appendix 11](#_Toc98507713)

[6.1 About Nessus 11](#_Toc98507714)

[6.1.1 Nessus vulnerabilities 11](#_Toc98507715)

[6.1.2 Nessus risk score 11](#_Toc98507716)

[6.2 About Burp Suite's web vulnerability scanner 13](#_Toc98507717)

[6.2.1 Burp Suite's web vulnerability scanner risk score 13](#_Toc98507718)

# Restrictions on disclosure and use of information

Restriction on Disclosure and Use of Confidential Information. The Executive understands and agrees that the Confidential Information constitutes an asset of the Company and its affiliated entities and may not be converted to the Executive's own use. Accordingly, the Executive hereby agrees that the Executive shall not, directly, or indirectly, at any time, reveal, divulge, or disclose to any Person not expressly authorized by the Company any Confidential Information, and the Executive shall not, directly, or indirectly, use or make use of any Confidential Information in connection with any business activity other than that of the Company. The parties acknowledge and agree that this Agreement is not intended to, and does not, alter either the Company's rights or the Executive's obligations under any state or federal statutory or common law regarding trade secrets and unfair trade.

# Operation Method

* 1. Posture Review
  2. Information Gathering
  3. Enumeration
  4. Vulnerability Assessment
  5. Analyze & Evaluate Risk Value
  6. Report



Figure 1: Operation Method

# Project Scope

## **3.1 Infrastructure Vulnerability Assessment**

**Target / IP Address:**

| **No.** | **Domain / Server Name** | **Public IP Address** | **Private IP Address** | **OS/Model** | **Functions** | **Public Assessment** | **Private Assessment** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | - | - | - | - | - | - | ✓ |

# Testing Tools

|  |  |
| --- | --- |
| **Tool Name** | **Testing Type** |
| Nmap | Host and Service Discovery |
| Nessus Professional | Infrastructure Vulnerability Assessment |
| Burp Suite's web vulnerability scanner | Web Application Vulnerability Assessment |

# Infrastructure Vulnerability Assessment

**Vulnerability Assessment from Public Access (for public target)**

**Testing date:** <<Date SCAN>>

**Tester IP Address:** <<IP Target>>

Diagram

Description automatically generated

Figure 2: Vulnerability Assessment from Public Access

**Vulnerability Assessment from Private Access (for private or restricted access target)**

**Testing date:** <<Date SCAN>>

**Tester IP Address:** Private IP from VPN access

A picture containing diagram

Description automatically generated

Figure 3: Vulnerability Assessment from Private Access

## **5.1 Target Information**

| **No.** | **Domain / Server Name** | **IP Address** | **OS/Model** | **Port** |
| --- | --- | --- | --- | --- |
| 1 | - | 83.118.33.130 | - | TCP: 80, 443, 8008, 8010 |
| 2 | - | 83.118.33.131 | - | TCP: 80, 443, 8008, 8010 |
| 3 | - | 83.118.33.132 | - | TCP: 53, 5061 |
| 4 | - | 83.118.33.135 | - | TCP: 80, 443, 8008, 8010 |
| 5 | - | 83.118.33.138 | - | TCP: 80, 443, 5000, 8008, 8010 |
| 6 | - | 83.118.33.144 | - | TCP: 80, 443, 3000, 8008, 8010 |
| 7 | - | 83.118.33.145 | - | TCP: 80, 443, 8008, 8010 |
| 8 | - | 83.118.33.148 | - | TCP: 80, 443, 8008, 8010 |
| 9 | - | 83.118.33.190 | - | TCP: 113 |
| 10 | - | 202.29.72.50 | - | TCP: 80, 443, 8008, 8010 |

## **5.2 Executive summary**

The purpose of this activity is to find the vulnerability on the target infrastructure.

### **5.2.1 Summary Vulnerability by Severity**

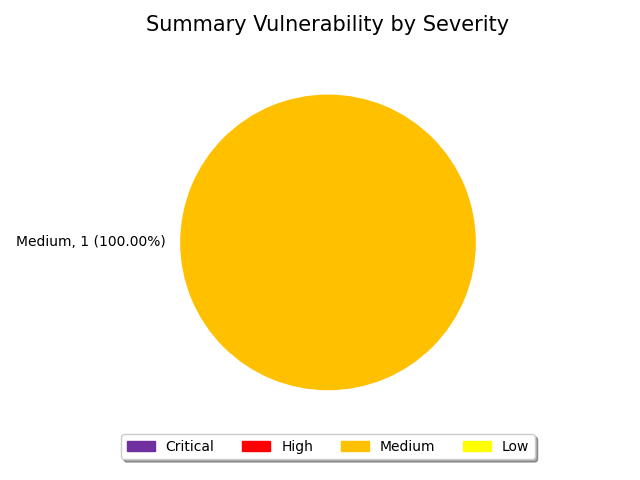


Figure 4: Summary by Severity of Infrastructure Vulnerability Assessment

### **5.2.2 Vulnerability by Target**

| **No.** | **Domain/Server Name** | **IP Address** | **Critical** | **High** | **Medium** | **Low** | **Total** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | - | 83.118.33.130 | 0 | 0 | 0 | 0 | 0 |
| 2 | - | 83.118.33.131 | 0 | 0 | 0 | 0 | 0 |
| 3 | - | 83.118.33.132 | 0 | 0 | 0 | 0 | 0 |
| 4 | - | 83.118.33.135 | 0 | 0 | 0 | 0 | 0 |
| 5 | - | 83.118.33.138 | 0 | 0 | 0 | 0 | 0 |
| 6 | - | 83.118.33.144 | 0 | 0 | 0 | 0 | 0 |
| 7 | - | 83.118.33.145 | 0 | 0 | 0 | 0 | 0 |
| 8 | - | 83.118.33.148 | 0 | 0 | 0 | 0 | 0 |
| 9 | - | 83.118.33.190 | 0 | 0 | 1 | 0 | 1 |
| 10 | - | 202.29.72.50 | 0 | 0 | 0 | 0 | 0 |
| **Total** | | | 0 | 0 | 1 | 0 | 1 |

## **5.3 Infrastructure Vulnerability Detail**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 1 | **Finding** | Internet Key Exchange (IKE) Aggressive Mode with Pre-Shared Key |
| **Severity** | **Medium** | **Port** | UDP: 500 |
| **Target** | 83.118.33.190(500) | | |
| **Detail** | The remote Internet Key Exchange (IKE) version 1 service seems to support Aggressive Mode with Pre-Shared key (PSK) authentication. Such a configuration could allow an attacker to capture and crack the PSK of a VPN gateway and gain unauthorized access to private networks. | | |
| **Solution** | - Disable Aggressive Mode if supported. - Do not use Pre-Shared key for authentication if it's possible. - If using Pre-Shared key cannot be avoided, use very strong keys. - If possible, do not allow VPN connections from any IP addresses.  Note that this plugin does not run over IPv6. | | |
| **Remark** | http://www.nessus.org/u?8d6444d2 https://www.ernw.de/download/pskattack.pdf http://www.nessus.org/u?d77bc12e https://www.securityfocus.com/bid/7423 | | |

# Appendix

## **6.1 About Nessus**

Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. Nessus is trusted by more than 30,000 organizations worldwide as one of the most widely deployed security technologies on the planet - and the gold standard for vulnerability assessment.

Reference: https://www.tenable.com/products/nessus

### **6.1.1 Nessus vulnerabilities**

As information about new vulnerabilities are discovered and released into the public domain, Tenable, Inc. research staff designs programs to enable Nessus to detect them. These programs are named plugins, and are written in the Nessus proprietary scripting language, called Nessus Attack Scripting Language (NASL). Plugins contain vulnerability information, a generic set of remediation actions, and the algorithm to test for the presence of the security issue.

Reference: https://www.tenable.com/plugins

### **6.1.2 Nessus risk score**

There are four risk levels in this document: Critical, High, Medium, and Low. There are methods for determining the risk level. Based on the Common Vulnerability Scoring System (CVSS), a standard for assessing the severity of vulnerabilities in computer systems. Regarded by the NIAC (National Infrastructure Advisory Council), expert assessments are measured in a range of 0 – 10

| **Severity** | **Description** | **Score** |
| --- | --- | --- |
| Critical | Vulnerabilities that score in the critical range usually have most of the following characteristics:   * Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices. * Exploitation is usually straightforward, in the sense that the attacker does not need any special authentication credentials or knowledge about individual victims, and does not need to persuade a target user, for example via social engineering, into performing any special functions.   For critical vulnerabilities, is advised that you patch or upgrade as soon as possible, unless you have other mitigating measures in place. For example, a mitigating factor could be if your installation is not accessible from the Internet. | 9.0 – 10.0 |
| High | Vulnerabilities that score in the high range usually have some of the following characteristics:   * The vulnerability is difficult to exploit. * Exploitation could result in elevated privileges. * Exploitation could result in a significant data loss or downtime. | 7.0 – 8.9 |
| Medium | Vulnerabilities that score in the medium range usually have some of the following characteristics:   * Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. * Denial of service vulnerabilities that are difficult to set up. * Exploits that require an attacker to reside on the same local network as the victim. * Vulnerabilities where exploitation provides only very limited access. * Vulnerabilities that require user privileges for successful exploitation. | 4.0 – 6.9 |
| Low | Vulnerabilities in the low range typically have very little impact on an organization's business. Exploitation of such vulnerabilities usually requires local or physical system access. | 0.1 – 3.9 |

## **6.2 About Burp Suite's web vulnerability scanner**

The web vulnerability scanner behind Burp Suite's popularity has more to it than most. Burp Scanner uses PortSwigger's world-leading research to help its users find a wide range of vulnerabilities in web applications, automatically. Sitting at the core of both Burp Suite Enterprise Edition and Burp Suite Professional, Burp Scanner is the weapon of choice for over 60,000 users across more than 15,000 organizations.

Reference: https://portswigger.net/burp/vulnerability-scanner

### **6.2.1 Burp Suite's web vulnerability scanner risk score**

The level of severity for an issue that was found by a scan. The higher the severity level, the larger the impact is likely to be if an attacker is able to exploit this vulnerability. Note that the severity level is only a rough approximation based on a typical website. You should use your knowledge of the purpose and context of the associated functionality to determine how serious each issue is in your individual case.

Reference: https://portswigger.net/burp/extensibility/enterprise/graphql-api/severity.html

| **Severity** | **Description** |
| --- | --- |
| High | An attacker can **fully** compromise the confidentiality, integrity, or availability, of a target system without specialized access, user interaction or circumstances that are beyond the attacker’s control. Very likely to allow lateral movement and escalation of attack to other systems on the internal network of the vulnerable application. |
| Medium | An attacker can **partially** compromise the confidentiality, integrity, or availability, of a target system. Specialized access, user interaction, or circumstances that are beyond the attacker’s control may be required for an attack to succeed. Very likely to be used in conjunction with other vulnerabilities to escalate an attack. |
| Low | An attacker can **limitedly** compromise the confidentiality, integrity, or availability, of a target system. Specialized access, user interaction, or circumstances that are beyond the attacker’s control is required for an attack to succeed. Needs to be used in conjunction with other vulnerabilities to escalate an attack. |