**รายงานสรุปผลการตรวจสอบช่องโหว่ของระบบ Nutanix Cloud**

**บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) ประจำปี 2565**

# วัตถุประสงค์

1. เพื่อค้นหาจุดอ่อนและช่องโหว่บนระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศของบริการ โดยใช้เทคนิคการตรวจสอบแบบ Vulnerability Assessment อ้างอิงจากมาตรฐาน Common Vulnerability Exposure, CVE และ Common Vulnerability Scoring System, CVSS-SIG
2. เพื่อนำเสนอข้อมูลจุดอ่อนหรือช่องโหว่ที่พบจากการตรวจสอบบนระบบโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศของบริการและเสนอแนะแนวทางในการแก้ไขจุดอ่อนและช่องโหว่ที่ตรวจพบ เพื่อให้ผู้ดูแลระบบเร่งดำเนินการแก้ไข

# เป้าหมาย

1. เพื่อให้ทราบถึงจุดอ่อนและช่องโหว่ของเครื่องที่ให้บริการ รวมถึงอุปกรณ์เครือข่ายภายในระบบสารสนเทศของบริการ
2. เพื่อนำเสนอข้อมูลจุดอ่อนหรือช่องโหว่ที่พบให้ ผู้ดูแลระบบ ผู้ดูแลเครือข่ายและผู้ดูแลระบบงานรับทราบถึงช่องโหว่ที่ตรวจพบเพื่อดำเนินการแก้ไข ปรับปรุงให้ระบบมีความแข็งแกร่งและยกระดับความมั่นคงปลอดภัยระบบสารสนเทศของบริการ

# แนวทางการประเมินความเสี่ยงที่พบ

การตรวจสอบจุดอ่อนและช่องโหว่ของเครื่องที่ให้บริการ และอุปกรณ์เครือข่ายภายในโครงสร้างระบบสารสนเทศ ดำเนินการตรวจสอบ โดยพิจารณาตามระดับความรุนแรงของจุดอ่อนและช่องโหว่ที่ตรวจพบ ซึ่งอ้างอิงตามมาตรฐาน Common Vulnerability Scoring System (CVSS) ที่ใช้เป็นมาตรฐานสากล โดยสามารถแบ่งระดับความรุนแรงของช่องโหว่ดังนี้

* **ความรุนแรงระดับวิกฤติ (CRITICAL)** หมายถึงจุดอ่อนหรือช่องโหว่ที่มีความเสี่ยงต่อการถูกบุกรุกระบบระดับวิกฤติ ผู้บุกรุกระบบสามารถใช้ช่องโหว่ที่ตรวจพบนี้โจมตีระบบได้ทันที และสร้างความเสียหายต่อระบบสารสนเทศในระดับวิกฤติ
* **ความรุนแรงระดับสูง (HIGH)** หมายถึงจุดอ่อนหรือช่องโหว่ที่มีความเสี่ยงต่อการถูกบุกรุกระบบระดับสูง ผู้บุกรุกระบบสามารถใช้ช่องโหว่ที่ตรวจพบนี้โจมตีระบบได้ทันที และสร้างความเสียหายต่อระบบสารสนเทศในระดับสูง
* **ความรุนแรงระดับกลาง (MEDIUM)** หมายถึงจุดอ่อนหรือช่องโหว่ที่มีความเสี่ยงต่อการถูกบุกรุกระบบระดับกลาง และผลกระทบของการบุกรุกระบบจะทำให้ระบบสารสนเทศมีความเสียหายในระดับกลาง
* **ความรุนแรงระดับต่ำ (LOW)** หมายถึงจุดอ่อนหรือช่องโหว่ที่มีความเสี่ยงต่อการถูกบุกรุกระบบระดับต่ำ และผลกระทบของการบุกรุกระบบทำให้ระบบสารสนเทศมีความเสียหายในระดับต่ำ
* **ไม่พบความรุนแรง (INFO)** หมายถึงรายละเอียดทั่วไปของระบบสารสนเทศ ซึ่งไม่มีผลกระทบต่อความเสียหายของระบบสารสนเทศ

**สารบัญ**

**หัวข้อ หน้า**

[วัตถุประสงค์ 1](#_Toc64730843)

[เป้าหมาย 1](#_Toc64730844)

[แนวทางการประเมินความเสี่ยงที่พบ 1](#_Toc64730845)

[ระยะเวลาในการดำเนินงาน 3](#_Toc64730846)

[รายงานสรุปผลการตรวจสอบ 3](#_Toc64730847)

[สรุปภาพโดยรวมช่องโหว่ที่ตรวจสอบพบบนระบบ Cloud Dell 4](#_Toc64730848)

[สรุปช่องโหว่พร้อมแนวทางแก้ไขโดยสังเขป 5](#_Toc64730849)

[ภาคผนวก รายละเอียดรายการ IP ที่ดำเนินการตรวจสอบช่องโหว่ 11](#_Toc64730850)

# ระยะเวลาในการดำเนินงาน

ดำเนินการตรวจสอบวิเคราะห์และประเมินความเสี่ยงของช่องโหว่ที่สำคัญ (Vulnerability Assessment) ของระบบ Nutanix Cloud จำนวน 616 รายการ ที่ บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน) อาคารไทยซัมมิททาวเวอร์ ชั้น 10 ในวันที่ 02 มีนาคม 2565 เวลา 19:30 น. – 21:00 น.

# รายงานสรุปผลการตรวจสอบ

รายงานสรุปผลการตรวจสอบนี้ใช้สำหรับผู้ดูแลระบบ การเตรียมความพร้อมในการแก้ไขช่องโหว่ที่ตรวจพบมีจุดประสงค์เพื่อลดความรุนแรงและผลกระทบจากการถูกบุกรุกผ่านช่องโหว่ดังกล่าว จากผลการตรวจสอบสรุปจำนวนช่องโหว่ตามระดับความเสี่ยงจากภายในเครือข่ายของแต่ละเครื่อง/อุปกรณ์ดังตารางด้านล่างนี้

| รายการอุปกรณ์ | จำนวน IP | Critical | High | Medium | Low | Info |
| --- | --- | --- | --- | --- | --- | --- |
| Nutanix Cloud | 616 | 10 | 7 | 1435 | 89 | 25409 |
| Summary | 616 | 10 | 7 | 1435 | 89 | 25409 |

**ตารางที่ 1** แสดงสรุปรายละเอียดผลการตรวจสอบช่องโหว่ที่ตรวจพบ

## สรุปภาพโดยรวมช่องโหว่ที่ตรวจสอบพบบนระบบ Nutanix Cloud

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | สรุปภาพรวมในการตรวจสอบช่องโหว่บนระบบ Nutanix Cloud  โดยมีเครื่องที่ให้บริการและอุปกรณ์เครือข่ายที่ได้รับการตรวจสอบ  ทั้งหมด จำนวน 616 รายการ   |  |  |  |  |  | | --- | --- | --- | --- | --- | | **ระดับความรุนแรง** | **CRITICAL** | **HIGH** | **MED** | **LOW** | | **เปอร์เซ็นต์** | 1% | 0% | 93% | 6% | | **จำนวนช่องโหว่** | 10 | 7 | 1435 | 89 | |

**ตารางที่ 2** แสดงภาพรวมช่องโหว่ที่ตรวจพบของระบบ Cloud Dell

## สรุปช่องโหว่พร้อมแนวทางแก้ไขโดยสังเขป

| ลำดับที่ | หมายเลขไอพี | รายละเอียดช่องโหว่ | ระดับความเสี่ยง | คำแนะนำในการแก้ไข |
| --- | --- | --- | --- | --- |
|  | 172.23.50.100 172.23.70.180 172.23.80.150 172.23.80.180 | VMware vCenter Server 6.5 / 6.7 Multiple Vulnerabilities (VMSA-2021-0027)  - The version of VMware vCenter Server installed on the remote host is 6.5 prior to 6.5 U3r or 6.7 prior to 6.7 U3p. It is, therefore, affected by multiple vulnerabilities:  - An arbitrary file read vulnerability exists in the vSphere web client. An unauthenticated, remote attacker  can exploit this, via HTTPS, to gain access to sensitive information. (CVE-2021-21980)  - A server side request forgery vulnerability exists in the vSAN Web Client plug-in. An unauthenticated,  remote attacker can exploit this, via HTTPS, to cause the server to access internal services or access  sites outside of vCenter. (CVE-2021-22049) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version  number. Nessus has also not tested for the presence of a workaround. | **Critical** | * Upgrade to VMware vCenter Server 6.5 U3r, 6.7 U3p, or later. |
|  | 172.23.90.3 172.23.90.11 172.23.90.51 172.23.90.52 172.23.90.53 172.23.90.60 | ESXi 6.5 / 6.7 XSS (VMSA-2020-0008)  - The remote VMware ESXi host is version 6.5 or 6.7 and is affected by a cross-site scripting (XSS) vulnerability in virtual machine attributes due to improper validation of user-supplied input before returning it to users. An authenticated, remote attacker with access to modify the system properties of a virtual machine from inside the guest OS can exploit this, by inserting script-related HTML in the system properties and having a user view the system properties from the ESXi Host Client, to execute arbitrary script code in a user's ESXi Host Client session.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | **Critical** | * Apply the appropriate patch as referenced in the vendor advisory. |
|  | 172.23.15.221 | SSL Medium Strength Cipher Suites Supported (SWEET32)  - The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or  else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network. | **High** | * Reconfigure the affected application if possible to avoid use of medium strength ciphers. |
|  | 172.23.90.3 172.23.90.11 172.23.90.51 172.23.90.52 172.23.90.53 172.23.90.60 | ESXi 6.5 / 6.7 / 7.0 Multiple Vulnerabilities (VMSA-2020-0026)  - According to its self-reported version number, the remote VMware ESXi host is version 6.5, 6.7 or 7.0 and is affected by multiple vulnerabilities.    - A use-after-free error exists in the XHCI USB controller. An unauthenticated, local attacker with local  administrative privileges on a virtual machine can exploit this, to execute code as the virtual machine's  VMX process running on the host. (CVE-2020-4004)   - A privilege escalation vulnerability exists in ESXi due to how certain system calls are managed. An  authenticated, local attacker with privileges within the VPM process can exploit this, when chained with  CVE-2020-4004, to obtain escalated privileges. (CVE-2020-4005)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | **High** | * Apply the appropriate patch as referenced in the vendor advisory. |
|  | 172.23.15.2 172.23.15.3 172.23.15.4 172.23.15.5 172.23.15.6 172.23.15.7 172.23.15.8 172.23.15.9 172.23.15.14 172.23.15.15 172.23.15.102 172.23.15.103 172.23.15.104 172.23.15.105 172.23.15.106 172.23.15.107 172.23.15.108 172.23.15.109 172.23.15.114 172.23.15.115 172.23.15.221 172.23.16.101 172.23.16.104 172.23.16.105 172.23.16.106 172.23.16.108 172.23.16.109 172.23.16.111 172.23.16.112 172.23.16.113 172.23.16.114 172.23.16.115 172.23.16.119 172.23.16.120 172.23.16.121 172.23.16.123 172.23.16.124 172.23.16.127 172.23.16.128 172.23.16.129 172.23.16.130 172.23.16.131 172.23.16.132 172.23.16.133 172.23.16.134 172.23.16.135 172.23.16.141 172.23.16.142 172.23.16.194 172.23.16.195 172.23.16.196 172.23.16.198 172.23.16.201 172.23.16.202 172.23.16.203 172.23.16.207 172.23.16.216 172.23.16.236 172.23.16.237 172.23.16.238 172.23.16.239 172.23.16.240 172.23.19.101 172.23.19.103 172.23.19.104 172.23.19.105 172.23.19.106 172.23.19.111 172.23.19.112 172.23.19.113 172.23.19.114 172.23.19.123 172.23.19.124 172.23.19.126 172.23.19.127 172.23.19.129 172.23.19.130 172.23.19.131 172.23.19.134 172.23.19.135 172.23.19.136 172.23.19.137 172.23.19.138 172.23.19.143 172.23.19.146 172.23.19.147 172.23.19.148 172.23.19.161 172.23.19.162 172.23.19.163 172.23.19.201 172.23.19.203 172.23.19.205 172.23.19.215 172.23.19.216 172.23.30.103 172.23.30.106 172.23.30.112 172.23.30.116 172.23.30.117 172.23.30.118 172.23.30.119 172.23.30.151 172.23.30.153 172.23.30.154 172.23.30.156 172.23.30.176 172.23.30.177 172.23.30.178 172.23.31.101 172.23.31.102 172.23.31.105 172.23.31.106 172.23.31.111 172.23.31.112 172.23.31.114 172.23.31.115 172.23.31.116 172.23.31.118 172.23.31.119 172.23.31.151 172.23.31.152 172.23.31.155 172.23.31.156 172.23.31.157 172.23.31.158 172.23.31.159 172.23.31.160 172.23.31.162 172.23.31.163 172.23.31.164 172.23.31.165 172.23.31.166 172.23.31.167 172.23.31.168 172.23.31.169 172.23.50.1 172.23.50.2 172.23.50.3 172.23.50.7 172.23.50.8 172.23.50.51 172.23.50.52 172.23.50.53 172.23.50.57 172.23.50.58 172.23.50.100 172.23.50.101 172.23.50.102 172.23.50.103 172.23.50.108 172.23.50.151 172.23.50.152 172.23.50.153 172.23.50.158 172.23.70.1 172.23.70.3 172.23.70.7 172.23.70.8 172.23.70.21 172.23.70.22 172.23.70.23 172.23.70.26 172.23.70.27 172.23.70.31 172.23.70.32 172.23.70.33 172.23.70.36 172.23.70.37 172.23.70.41 172.23.70.42 172.23.70.43 172.23.70.44 172.23.70.45 172.23.70.47 172.23.70.48 172.23.70.51 172.23.70.52 172.23.70.53 172.23.70.54 172.23.70.57 172.23.70.58 172.23.70.88 172.23.70.89 172.23.70.90 172.23.70.91 172.23.70.92 172.23.70.93 172.23.70.94 172.23.70.95 172.23.70.96 172.23.70.100 172.23.70.102 172.23.70.103 172.23.70.122 172.23.70.126 172.23.70.127 172.23.70.131 172.23.70.132 172.23.70.136 172.23.70.137 172.23.70.141 172.23.70.143 172.23.70.144 172.23.70.145 172.23.70.148 172.23.70.150 172.23.70.152 172.23.70.157 172.23.70.158 172.23.70.180 172.23.70.188 172.23.70.189 172.23.70.190 172.23.70.191 172.23.70.193 172.23.70.194 172.23.70.195 172.23.70.201 172.23.70.202 172.23.70.203 172.23.70.205 172.23.70.206 172.23.80.1 172.23.80.2 172.23.80.3 172.23.80.7 172.23.80.8 172.23.80.11 172.23.80.12 172.23.80.13 172.23.80.14 172.23.80.31 172.23.80.32 172.23.80.33 172.23.80.34 172.23.80.35 172.23.80.36 172.23.80.37 172.23.80.38 172.23.80.39 172.23.80.51 172.23.80.52 172.23.80.53 172.23.80.57 172.23.80.58 172.23.80.71 172.23.80.72 172.23.80.73 172.23.80.74 172.23.80.81 172.23.80.82 172.23.80.83 172.23.80.84 172.23.80.85 172.23.80.86 172.23.80.87 172.23.80.88 172.23.80.89 172.23.80.100 172.23.80.101 172.23.80.102 172.23.80.103 172.23.80.107 172.23.80.108 172.23.80.111 172.23.80.112 172.23.80.113 172.23.80.114 172.23.80.131 172.23.80.132 172.23.80.133 172.23.80.134 172.23.80.135 172.23.80.137 172.23.80.138 172.23.80.139 172.23.80.150 172.23.80.151 172.23.80.152 172.23.80.153 172.23.80.157 172.23.80.158 172.23.80.171 172.23.80.172 172.23.80.173 172.23.80.174 172.23.80.180 172.23.80.181 172.23.80.182 172.23.80.183 172.23.80.184 172.23.80.185 172.23.80.186 172.23.80.187 172.23.80.188 172.23.80.189 172.23.80.201 172.23.80.202 172.23.80.203 172.23.80.204 172.23.80.205 172.23.80.206 172.23.90.1 172.23.90.2 172.23.90.3 172.23.90.6 172.23.90.7 172.23.90.8 172.23.90.10 172.23.90.11 172.23.90.12 172.23.90.13 172.23.90.21 172.23.90.22 172.23.90.23 172.23.90.24 172.23.90.25 172.23.90.26 172.23.90.27 172.23.90.28 172.23.90.29 172.23.90.51 172.23.90.52 172.23.90.53 172.23.90.54 172.23.90.55 172.23.90.56 172.23.90.60 172.23.90.61 172.23.90.62 172.23.90.63 172.23.90.91 172.23.90.92 172.23.90.93 172.23.90.94 172.23.90.95 172.23.90.100 172.23.90.101 172.23.90.102 172.23.90.103 172.23.90.106 172.23.90.107 172.23.90.108 172.23.90.110 172.23.90.111 172.23.90.112 172.23.90.113 172.23.90.121 172.23.90.122 172.23.90.123 172.23.90.124 172.23.90.125 172.23.90.126 172.23.90.127 172.23.90.129 172.23.90.150 172.23.90.151 172.23.90.152 172.23.90.153 172.23.90.154 172.23.90.155 172.23.90.156 172.23.90.160 172.23.90.161 172.23.90.162 172.23.90.163 172.23.90.192 172.23.90.193 172.23.90.194 172.23.90.195 172.23.90.203 172.23.90.204 172.23.90.206 172.24.20.101 172.24.20.102 172.24.20.103 172.24.20.104 172.24.20.105 172.24.20.106 172.24.20.107 172.24.20.108 172.24.20.109 172.24.20.151 172.24.20.152 172.24.20.153 172.24.20.154 172.24.20.155 172.24.20.156 172.24.20.157 172.24.20.158 172.24.20.159 172.24.20.201 172.24.20.202 | SSL Certificate Cannot Be Trusted  - The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :   - First, the top of the certificate chain sent by the  server might not be descended from a known public  certificate authority. This can occur either when the  top of the chain is an unrecognized, self-signed  certificate, or when intermediate certificates are  missing that would connect the top of the certificate  chain to a known public certificate authority.   - Second, the certificate chain may contain a certificate  that is not valid at the time of the scan. This can  occur either when the scan occurs before one of the  certificate's 'notBefore' dates, or after one of the  certificate's 'notAfter' dates.   - Third, the certificate chain may contain a signature  that either didn't match the certificate's information  or could not be verified. Bad signatures can be fixed by  getting the certificate with the bad signature to be  re-signed by its issuer. Signatures that could not be  verified are the result of the certificate's issuer  using a signing algorithm that Nessus either does not  support or does not recognize.  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and  identity of the web server. This could make it easier to carry out  man-in-the-middle attacks against the remote host. | **Medium** | * Purchase or generate a proper SSL certificate for this service. |
|  | 172.23.15.2 172.23.15.3 172.23.15.4 172.23.15.5 172.23.15.6 172.23.15.7 172.23.15.8 172.23.15.9 172.23.15.14 172.23.15.15 172.23.15.102 172.23.15.103 172.23.15.104 172.23.15.105 172.23.15.106 172.23.15.107 172.23.15.108 172.23.15.109 172.23.15.114 172.23.15.115 172.23.15.221 172.23.16.101 172.23.16.104 172.23.16.105 172.23.16.106 172.23.16.108 172.23.16.109 172.23.16.111 172.23.16.112 172.23.16.113 172.23.16.114 172.23.16.115 172.23.16.119 172.23.16.120 172.23.16.121 172.23.16.123 172.23.16.124 172.23.16.127 172.23.16.128 172.23.16.129 172.23.16.130 172.23.16.131 172.23.16.132 172.23.16.133 172.23.16.134 172.23.16.135 172.23.16.141 172.23.16.142 172.23.16.194 172.23.16.195 172.23.16.196 172.23.16.198 172.23.16.201 172.23.16.202 172.23.16.203 172.23.16.207 172.23.16.216 172.23.16.236 172.23.16.237 172.23.16.238 172.23.16.239 172.23.16.240 172.23.19.101 172.23.19.103 172.23.19.104 172.23.19.105 172.23.19.106 172.23.19.111 172.23.19.112 172.23.19.113 172.23.19.114 172.23.19.123 172.23.19.124 172.23.19.126 172.23.19.127 172.23.19.129 172.23.19.130 172.23.19.131 172.23.19.134 172.23.19.135 172.23.19.136 172.23.19.137 172.23.19.138 172.23.19.143 172.23.19.146 172.23.19.147 172.23.19.148 172.23.19.161 172.23.19.162 172.23.19.163 172.23.19.201 172.23.19.203 172.23.19.205 172.23.19.215 172.23.19.216 172.23.30.103 172.23.30.106 172.23.30.112 172.23.30.116 172.23.30.117 172.23.30.118 172.23.30.119 172.23.30.151 172.23.30.153 172.23.30.154 172.23.30.156 172.23.30.176 172.23.30.177 172.23.30.178 172.23.31.101 172.23.31.102 172.23.31.105 172.23.31.106 172.23.31.111 172.23.31.112 172.23.31.114 172.23.31.115 172.23.31.116 172.23.31.118 172.23.31.119 172.23.31.151 172.23.31.152 172.23.31.155 172.23.31.156 172.23.31.157 172.23.31.158 172.23.31.159 172.23.31.160 172.23.31.162 172.23.31.163 172.23.31.164 172.23.31.165 172.23.31.166 172.23.31.167 172.23.31.168 172.23.31.169 172.23.50.1 172.23.50.2 172.23.50.3 172.23.50.7 172.23.50.8 172.23.50.51 172.23.50.52 172.23.50.53 172.23.50.57 172.23.50.58 172.23.50.101 172.23.50.102 172.23.50.103 172.23.50.108 172.23.50.151 172.23.50.152 172.23.50.153 172.23.50.158 172.23.70.1 172.23.70.3 172.23.70.7 172.23.70.8 172.23.70.21 172.23.70.22 172.23.70.23 172.23.70.26 172.23.70.27 172.23.70.31 172.23.70.32 172.23.70.33 172.23.70.36 172.23.70.37 172.23.70.41 172.23.70.42 172.23.70.43 172.23.70.44 172.23.70.45 172.23.70.47 172.23.70.48 172.23.70.51 172.23.70.52 172.23.70.53 172.23.70.54 172.23.70.57 172.23.70.58 172.23.70.88 172.23.70.89 172.23.70.90 172.23.70.91 172.23.70.92 172.23.70.93 172.23.70.94 172.23.70.95 172.23.70.96 172.23.70.102 172.23.70.103 172.23.70.122 172.23.70.126 172.23.70.127 172.23.70.131 172.23.70.132 172.23.70.136 172.23.70.137 172.23.70.141 172.23.70.143 172.23.70.144 172.23.70.145 172.23.70.148 172.23.70.152 172.23.70.157 172.23.70.158 172.23.70.188 172.23.70.189 172.23.70.190 172.23.70.191 172.23.70.193 172.23.70.194 172.23.70.195 172.23.70.201 172.23.70.202 172.23.70.203 172.23.70.205 172.23.70.206 172.23.80.1 172.23.80.2 172.23.80.3 172.23.80.7 172.23.80.8 172.23.80.11 172.23.80.12 172.23.80.13 172.23.80.14 172.23.80.31 172.23.80.32 172.23.80.33 172.23.80.34 172.23.80.35 172.23.80.36 172.23.80.37 172.23.80.38 172.23.80.39 172.23.80.51 172.23.80.52 172.23.80.53 172.23.80.57 172.23.80.58 172.23.80.71 172.23.80.72 172.23.80.73 172.23.80.74 172.23.80.81 172.23.80.82 172.23.80.83 172.23.80.84 172.23.80.85 172.23.80.86 172.23.80.87 172.23.80.88 172.23.80.89 172.23.80.101 172.23.80.102 172.23.80.103 172.23.80.107 172.23.80.108 172.23.80.111 172.23.80.112 172.23.80.113 172.23.80.114 172.23.80.131 172.23.80.132 172.23.80.133 172.23.80.134 172.23.80.135 172.23.80.137 172.23.80.138 172.23.80.139 172.23.80.151 172.23.80.152 172.23.80.153 172.23.80.157 172.23.80.158 172.23.80.171 172.23.80.172 172.23.80.173 172.23.80.174 172.23.80.181 172.23.80.182 172.23.80.183 172.23.80.184 172.23.80.185 172.23.80.186 172.23.80.187 172.23.80.188 172.23.80.189 172.23.80.201 172.23.80.202 172.23.80.203 172.23.80.204 172.23.80.205 172.23.80.206 172.23.90.1 172.23.90.2 172.23.90.3 172.23.90.6 172.23.90.7 172.23.90.8 172.23.90.10 172.23.90.11 172.23.90.12 172.23.90.13 172.23.90.21 172.23.90.22 172.23.90.23 172.23.90.24 172.23.90.25 172.23.90.26 172.23.90.27 172.23.90.28 172.23.90.29 172.23.90.51 172.23.90.52 172.23.90.53 172.23.90.54 172.23.90.55 172.23.90.56 172.23.90.60 172.23.90.61 172.23.90.62 172.23.90.63 172.23.90.91 172.23.90.92 172.23.90.93 172.23.90.94 172.23.90.95 172.23.90.101 172.23.90.102 172.23.90.103 172.23.90.106 172.23.90.107 172.23.90.108 172.23.90.110 172.23.90.111 172.23.90.112 172.23.90.113 172.23.90.121 172.23.90.122 172.23.90.123 172.23.90.124 172.23.90.125 172.23.90.126 172.23.90.127 172.23.90.129 172.23.90.151 172.23.90.152 172.23.90.153 172.23.90.154 172.23.90.155 172.23.90.156 172.23.90.160 172.23.90.161 172.23.90.162 172.23.90.163 172.23.90.192 172.23.90.193 172.23.90.194 172.23.90.195 172.23.90.203 172.23.90.204 172.23.90.206 172.24.20.101 172.24.20.102 172.24.20.103 172.24.20.104 172.24.20.105 172.24.20.106 172.24.20.107 172.24.20.108 172.24.20.109 172.24.20.151 172.24.20.152 172.24.20.153 172.24.20.154 172.24.20.155 172.24.20.156 172.24.20.157 172.24.20.158 172.24.20.159 172.24.20.201 172.24.20.202 | SSL Self-Signed Certificate  - The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.   Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. | **Medium** | * Purchase or generate a proper SSL certificate for this service. |
|  | 172.23.15.221 | SSL RC4 Cipher Suites Supported (Bar Mitzvah)  - The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness. If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext. | **Medium** | * Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support. |
|  | 172.23.15.221 | TLS Version 1.0 Protocol Detection  - The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible. As of March 31, 2020, Endpoints that aren’t enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits. | **Medium** | * Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0. |
|  | 172.23.16.101 172.23.16.104 172.23.16.105 172.23.16.106 172.23.16.114 172.23.16.115 172.23.16.119 172.23.16.120 172.23.16.121 172.23.16.124 172.23.16.127 172.23.16.130 172.23.16.131 172.23.16.132 172.23.16.133 172.23.16.134 172.23.16.135 172.23.16.141 172.23.16.142 172.23.16.198 172.23.16.201 172.23.16.202 172.23.16.207 172.23.16.236 172.23.16.237 172.23.16.238 172.23.16.239 172.23.16.240 172.23.19.101 172.23.19.104 172.23.19.105 172.23.19.106 172.23.19.111 172.23.19.112 172.23.19.113 172.23.19.114 172.23.19.123 172.23.19.124 172.23.19.126 172.23.19.127 172.23.19.129 172.23.19.130 172.23.19.131 172.23.19.134 172.23.19.135 172.23.19.136 172.23.19.137 172.23.19.138 172.23.19.148 172.23.19.201 172.23.19.203 172.23.19.215 172.23.19.216 | SSL Certificate Expiry  - This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired. | **Medium** | * Purchase or generate a new SSL certificate to replace the existing one. |
|  | 172.23.90.3 172.23.90.11 172.23.90.51 172.23.90.52 172.23.90.53 172.23.90.60 | ESXi 6.5 / 6.7 / 7.0 DoS (VMSA-2020-0018)  - The remote VMware ESXi host is version 6.5, 6.7 or 7.0 and is affected by a denial of service (DoS) vulnerability in the authentication service. An unauthenticated, remote attacker can exploit this issue to exhaust memory resources  resulting in a degradation of performance condition while the attack is sustained.  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | **Medium** | * Apply the appropriate patch as referenced in the vendor advisory. |
|  | 172.23.16.1 172.23.16.4 172.23.16.5 172.23.16.6 172.23.16.8 172.23.16.9 172.23.16.16 172.23.16.23 172.23.16.24 172.23.16.27 172.23.16.28 172.23.16.29 172.23.16.30 172.23.16.31 172.23.16.32 172.23.16.33 172.23.16.34 172.23.16.35 172.23.16.41 172.23.16.42 172.23.16.51 172.23.16.52 172.23.16.53 172.23.16.54 172.23.16.55 172.23.16.59 172.23.16.60 172.23.16.61 172.23.16.94 172.23.16.95 172.23.16.96 172.23.16.107 172.23.16.136 172.23.16.137 172.23.16.138 172.23.16.139 172.23.16.140 172.23.16.197 172.23.19.1 172.23.19.2 172.23.19.3 172.23.19.4 172.23.19.5 172.23.19.6 172.23.19.7 172.23.19.8 172.23.19.9 172.23.19.10 172.23.19.11 172.23.19.12 172.23.19.13 172.23.19.14 172.23.19.20 172.23.19.21 172.23.19.22 172.23.19.23 172.23.19.24 172.23.19.26 172.23.19.27 172.23.19.34 172.23.19.36 172.23.19.37 172.23.19.38 172.23.19.43 172.23.19.44 172.23.19.46 172.23.19.47 172.23.19.61 172.23.19.63 172.23.19.115 172.23.19.116 172.23.30.1 172.23.30.2 172.23.30.3 172.23.30.4 172.23.30.5 172.23.30.6 172.23.30.51 172.23.30.52 172.23.30.53 172.23.30.54 172.23.31.5 172.23.31.6 172.23.31.51 172.23.31.52 172.23.31.55 172.23.31.56 172.23.31.57 172.23.31.60 | SSH Weak Key Exchange Algorithms Enabled  - The remote SSH server is configured to allow key exchange algorithms which are considered weak.  This is based on the IETF draft document Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) draft-ietf-curdle-ssh-kex-sha2-20. Section 4 lists guidance on key exchange algorithms that SHOULD NOT and MUST NOT be enabled. This includes:   diffie-hellman-group-exchange-sha1   diffie-hellman-group1-sha1   gss-gex-sha1-\*   gss-group1-sha1-\*   gss-group14-sha1-\*   rsa1024-sha1  Note that this plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions. | **Low** | * Contact the vendor or consult product documentation to disable the weak algorithms. |

**ตารางที่ 3** รายละเอียดช่องโหว่พร้อมแนวทางการแก้ไข

## ภาคผนวก รายละเอียดรายการ IP ที่ดำเนินการตรวจสอบช่องโหว่

| * Nutanix Cloud |
| --- |

| 172.23.15.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 172.23.15.2 | 0 | 0 | 7 | 0 | 7 |
| 2. | 172.23.15.3 | 0 | 0 | 7 | 0 | 7 |
| 3. | 172.23.15.4 | 0 | 0 | 7 | 0 | 7 |
| 4. | 172.23.15.5 | 0 | 0 | 7 | 0 | 7 |
| 5. | 172.23.15.6 | 0 | 0 | 7 | 0 | 7 |
| 6. | 172.23.15.7 | 0 | 0 | 7 | 0 | 7 |
| 7. | 172.23.15.8 | 0 | 0 | 7 | 0 | 7 |
| 8. | 172.23.15.9 | 0 | 0 | 7 | 0 | 7 |
| 9. | 172.23.15.14 | 0 | 0 | 7 | 0 | 7 |
| 10. | 172.23.15.15 | 0 | 0 | 7 | 0 | 7 |
| 11. | 172.23.15.102 | 0 | 0 | 2 | 0 | 2 |
| 12. | 172.23.15.103 | 0 | 0 | 2 | 0 | 2 |
| 13. | 172.23.15.104 | 0 | 0 | 2 | 0 | 2 |
| 14. | 172.23.15.105 | 0 | 0 | 2 | 0 | 2 |
| 15. | 172.23.15.106 | 0 | 0 | 2 | 0 | 2 |
| 16. | 172.23.15.107 | 0 | 0 | 2 | 0 | 2 |
| 17. | 172.23.15.108 | 0 | 0 | 2 | 0 | 2 |
| 18. | 172.23.15.109 | 0 | 0 | 2 | 0 | 2 |
| 19. | 172.23.15.114 | 0 | 0 | 2 | 0 | 2 |
| 20. | 172.23.15.115 | 0 | 0 | 2 | 0 | 2 |
| 21. | 172.23.15.221 | 0 | 1 | 4 | 0 | 5 |
| Summary | | 0 | 1 | 94 | 0 | 95 |

| 172.23.16.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 172.23.16.1 | 0 | 0 | 0 | 1 | 1 |
| 2. | 172.23.16.4 | 0 | 0 | 0 | 1 | 1 |
| 3. | 172.23.16.5 | 0 | 0 | 0 | 1 | 1 |
| 4. | 172.23.16.6 | 0 | 0 | 0 | 1 | 1 |
| 5. | 172.23.16.8 | 0 | 0 | 0 | 1 | 1 |
| 6. | 172.23.16.9 | 0 | 0 | 0 | 1 | 1 |
| 7. | 172.23.16.16 | 0 | 0 | 0 | 1 | 1 |
| 8. | 172.23.16.23 | 0 | 0 | 0 | 1 | 1 |
| 9. | 172.23.16.24 | 0 | 0 | 0 | 1 | 1 |
| 10. | 172.23.16.27 | 0 | 0 | 0 | 1 | 1 |
| 11. | 172.23.16.28 | 0 | 0 | 0 | 1 | 1 |
| 12. | 172.23.16.29 | 0 | 0 | 0 | 1 | 1 |
| 13. | 172.23.16.30 | 0 | 0 | 0 | 1 | 1 |
| 14. | 172.23.16.31 | 0 | 0 | 0 | 1 | 1 |
| 15. | 172.23.16.32 | 0 | 0 | 0 | 1 | 1 |
| 16. | 172.23.16.33 | 0 | 0 | 0 | 1 | 1 |
| 17. | 172.23.16.34 | 0 | 0 | 0 | 1 | 1 |
| 18. | 172.23.16.35 | 0 | 0 | 0 | 1 | 1 |
| 19. | 172.23.16.41 | 0 | 0 | 0 | 1 | 1 |
| 20. | 172.23.16.42 | 0 | 0 | 0 | 1 | 1 |
| 21. | 172.23.16.51 | 0 | 0 | 0 | 1 | 1 |
| 22. | 172.23.16.52 | 0 | 0 | 0 | 1 | 1 |
| 23. | 172.23.16.53 | 0 | 0 | 0 | 1 | 1 |
| 24. | 172.23.16.54 | 0 | 0 | 0 | 1 | 1 |
| 25. | 172.23.16.55 | 0 | 0 | 0 | 1 | 1 |
| 26. | 172.23.16.59 | 0 | 0 | 0 | 1 | 1 |
| 27. | 172.23.16.60 | 0 | 0 | 0 | 1 | 1 |
| 28. | 172.23.16.61 | 0 | 0 | 0 | 1 | 1 |
| 29. | 172.23.16.94 | 0 | 0 | 0 | 1 | 1 |
| 30. | 172.23.16.95 | 0 | 0 | 0 | 1 | 1 |
| 31. | 172.23.16.96 | 0 | 0 | 0 | 1 | 1 |
| 32. | 172.23.16.101 | 0 | 0 | 3 | 0 | 3 |
| 33. | 172.23.16.104 | 0 | 0 | 3 | 0 | 3 |
| 34. | 172.23.16.105 | 0 | 0 | 3 | 0 | 3 |
| 35. | 172.23.16.106 | 0 | 0 | 3 | 0 | 3 |
| 36. | 172.23.16.107 | 0 | 0 | 0 | 1 | 1 |
| 37. | 172.23.16.108 | 0 | 0 | 2 | 0 | 2 |
| 38. | 172.23.16.109 | 0 | 0 | 2 | 0 | 2 |
| 39. | 172.23.16.111 | 0 | 0 | 2 | 0 | 2 |
| 40. | 172.23.16.112 | 0 | 0 | 2 | 0 | 2 |
| 41. | 172.23.16.113 | 0 | 0 | 2 | 0 | 2 |
| 42. | 172.23.16.114 | 0 | 0 | 3 | 0 | 3 |
| 43. | 172.23.16.115 | 0 | 0 | 3 | 0 | 3 |
| 44. | 172.23.16.119 | 0 | 0 | 3 | 0 | 3 |
| 45. | 172.23.16.120 | 0 | 0 | 3 | 0 | 3 |
| 46. | 172.23.16.121 | 0 | 0 | 3 | 0 | 3 |
| 47. | 172.23.16.123 | 0 | 0 | 2 | 0 | 2 |
| 48. | 172.23.16.124 | 0 | 0 | 3 | 0 | 3 |
| 49. | 172.23.16.127 | 0 | 0 | 3 | 0 | 3 |
| 50. | 172.23.16.128 | 0 | 0 | 2 | 0 | 2 |
| 51. | 172.23.16.129 | 0 | 0 | 2 | 0 | 2 |
| 52. | 172.23.16.130 | 0 | 0 | 3 | 0 | 3 |
| 53. | 172.23.16.131 | 0 | 0 | 3 | 0 | 3 |
| 54. | 172.23.16.132 | 0 | 0 | 3 | 0 | 3 |
| 55. | 172.23.16.133 | 0 | 0 | 3 | 0 | 3 |
| 56. | 172.23.16.134 | 0 | 0 | 3 | 0 | 3 |
| 57. | 172.23.16.135 | 0 | 0 | 3 | 0 | 3 |
| 58. | 172.23.16.136 | 0 | 0 | 0 | 1 | 1 |
| 59. | 172.23.16.137 | 0 | 0 | 0 | 1 | 1 |
| 60. | 172.23.16.138 | 0 | 0 | 0 | 1 | 1 |
| 61. | 172.23.16.139 | 0 | 0 | 0 | 1 | 1 |
| 62. | 172.23.16.140 | 0 | 0 | 0 | 1 | 1 |
| 63. | 172.23.16.141 | 0 | 0 | 3 | 0 | 3 |
| 64. | 172.23.16.142 | 0 | 0 | 3 | 0 | 3 |
| 65. | 172.23.16.194 | 0 | 0 | 2 | 0 | 2 |
| 66. | 172.23.16.195 | 0 | 0 | 2 | 0 | 2 |
| 67. | 172.23.16.196 | 0 | 0 | 2 | 0 | 2 |
| 68. | 172.23.16.197 | 0 | 0 | 0 | 1 | 1 |
| 69. | 172.23.16.198 | 0 | 0 | 3 | 0 | 3 |
| 70. | 172.23.16.201 | 0 | 0 | 3 | 0 | 3 |
| 71. | 172.23.16.202 | 0 | 0 | 3 | 0 | 3 |
| 72. | 172.23.16.203 | 0 | 0 | 2 | 0 | 2 |
| 73. | 172.23.16.207 | 0 | 0 | 3 | 0 | 3 |
| 74. | 172.23.16.216 | 0 | 0 | 2 | 0 | 2 |
| 75. | 172.23.16.236 | 0 | 0 | 3 | 0 | 3 |
| 76. | 172.23.16.237 | 0 | 0 | 3 | 0 | 3 |
| 77. | 172.23.16.238 | 0 | 0 | 3 | 0 | 3 |
| 78. | 172.23.16.239 | 0 | 0 | 3 | 0 | 3 |
| 79. | 172.23.16.240 | 0 | 0 | 3 | 0 | 3 |
| Summary | | 0 | 0 | 110 | 38 | 148 |

| 172.23.19.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 172.23.19.1 | 0 | 0 | 0 | 1 | 1 |
| 2. | 172.23.19.2 | 0 | 0 | 0 | 1 | 1 |
| 3. | 172.23.19.3 | 0 | 0 | 0 | 1 | 1 |
| 4. | 172.23.19.4 | 0 | 0 | 0 | 1 | 1 |
| 5. | 172.23.19.5 | 0 | 0 | 0 | 1 | 1 |
| 6. | 172.23.19.6 | 0 | 0 | 0 | 1 | 1 |
| 7. | 172.23.19.7 | 0 | 0 | 0 | 1 | 1 |
| 8. | 172.23.19.8 | 0 | 0 | 0 | 1 | 1 |
| 9. | 172.23.19.9 | 0 | 0 | 0 | 1 | 1 |
| 10. | 172.23.19.10 | 0 | 0 | 0 | 1 | 1 |
| 11. | 172.23.19.11 | 0 | 0 | 0 | 1 | 1 |
| 12. | 172.23.19.12 | 0 | 0 | 0 | 1 | 1 |
| 13. | 172.23.19.13 | 0 | 0 | 0 | 1 | 1 |
| 14. | 172.23.19.14 | 0 | 0 | 0 | 1 | 1 |
| 15. | 172.23.19.20 | 0 | 0 | 0 | 1 | 1 |
| 16. | 172.23.19.21 | 0 | 0 | 0 | 1 | 1 |
| 17. | 172.23.19.22 | 0 | 0 | 0 | 1 | 1 |
| 18. | 172.23.19.23 | 0 | 0 | 0 | 1 | 1 |
| 19. | 172.23.19.24 | 0 | 0 | 0 | 1 | 1 |
| 20. | 172.23.19.25 | 0 | 0 | 0 | 0 | 0 |
| 21. | 172.23.19.26 | 0 | 0 | 0 | 1 | 1 |
| 22. | 172.23.19.27 | 0 | 0 | 0 | 1 | 1 |
| 23. | 172.23.19.28 | 0 | 0 | 0 | 0 | 0 |
| 24. | 172.23.19.29 | 0 | 0 | 0 | 0 | 0 |
| 25. | 172.23.19.30 | 0 | 0 | 0 | 0 | 0 |
| 26. | 172.23.19.31 | 0 | 0 | 0 | 0 | 0 |
| 27. | 172.23.19.32 | 0 | 0 | 0 | 0 | 0 |
| 28. | 172.23.19.33 | 0 | 0 | 0 | 0 | 0 |
| 29. | 172.23.19.34 | 0 | 0 | 0 | 1 | 1 |
| 30. | 172.23.19.35 | 0 | 0 | 0 | 0 | 0 |
| 31. | 172.23.19.36 | 0 | 0 | 0 | 1 | 1 |
| 32. | 172.23.19.37 | 0 | 0 | 0 | 1 | 1 |
| 33. | 172.23.19.38 | 0 | 0 | 0 | 1 | 1 |
| 34. | 172.23.19.43 | 0 | 0 | 0 | 1 | 1 |
| 35. | 172.23.19.44 | 0 | 0 | 0 | 1 | 1 |
| 36. | 172.23.19.45 | 0 | 0 | 0 | 0 | 0 |
| 37. | 172.23.19.46 | 0 | 0 | 0 | 1 | 1 |
| 38. | 172.23.19.47 | 0 | 0 | 0 | 1 | 1 |
| 39. | 172.23.19.48 | 0 | 0 | 0 | 0 | 0 |
| 40. | 172.23.19.61 | 0 | 0 | 0 | 1 | 1 |
| 41. | 172.23.19.62 | 0 | 0 | 0 | 0 | 0 |
| 42. | 172.23.19.63 | 0 | 0 | 0 | 1 | 1 |
| 43. | 172.23.19.64 | 0 | 0 | 0 | 0 | 0 |
| 44. | 172.23.19.101 | 0 | 0 | 3 | 0 | 3 |
| 45. | 172.23.19.102 | 0 | 0 | 0 | 0 | 0 |
| 46. | 172.23.19.103 | 0 | 0 | 2 | 0 | 2 |
| 47. | 172.23.19.104 | 0 | 0 | 3 | 0 | 3 |
| 48. | 172.23.19.105 | 0 | 0 | 3 | 0 | 3 |
| 49. | 172.23.19.106 | 0 | 0 | 3 | 0 | 3 |
| 50. | 172.23.19.107 | 0 | 0 | 0 | 0 | 0 |
| 51. | 172.23.19.108 | 0 | 0 | 0 | 0 | 0 |
| 52. | 172.23.19.109 | 0 | 0 | 0 | 0 | 0 |
| 53. | 172.23.19.110 | 0 | 0 | 0 | 0 | 0 |
| 54. | 172.23.19.111 | 0 | 0 | 3 | 0 | 3 |
| 55. | 172.23.19.112 | 0 | 0 | 3 | 0 | 3 |
| 56. | 172.23.19.113 | 0 | 0 | 3 | 0 | 3 |
| 57. | 172.23.19.114 | 0 | 0 | 3 | 0 | 3 |
| 58. | 172.23.19.115 | 0 | 0 | 0 | 1 | 1 |
| 59. | 172.23.19.116 | 0 | 0 | 0 | 1 | 1 |
| 60. | 172.23.19.120 | 0 | 0 | 0 | 0 | 0 |
| 61. | 172.23.19.121 | 0 | 0 | 0 | 0 | 0 |
| 62. | 172.23.19.122 | 0 | 0 | 0 | 0 | 0 |
| 63. | 172.23.19.123 | 0 | 0 | 3 | 0 | 3 |
| 64. | 172.23.19.124 | 0 | 0 | 3 | 0 | 3 |
| 65. | 172.23.19.125 | 0 | 0 | 0 | 0 | 0 |
| 66. | 172.23.19.126 | 0 | 0 | 3 | 0 | 3 |
| 67. | 172.23.19.127 | 0 | 0 | 3 | 0 | 3 |
| 68. | 172.23.19.128 | 0 | 0 | 0 | 0 | 0 |
| 69. | 172.23.19.129 | 0 | 0 | 3 | 0 | 3 |
| 70. | 172.23.19.130 | 0 | 0 | 3 | 0 | 3 |
| 71. | 172.23.19.131 | 0 | 0 | 3 | 0 | 3 |
| 72. | 172.23.19.132 | 0 | 0 | 0 | 0 | 0 |
| 73. | 172.23.19.133 | 0 | 0 | 0 | 0 | 0 |
| 74. | 172.23.19.134 | 0 | 0 | 3 | 0 | 3 |
| 75. | 172.23.19.135 | 0 | 0 | 3 | 0 | 3 |
| 76. | 172.23.19.136 | 0 | 0 | 3 | 0 | 3 |
| 77. | 172.23.19.137 | 0 | 0 | 3 | 0 | 3 |
| 78. | 172.23.19.138 | 0 | 0 | 3 | 0 | 3 |
| 79. | 172.23.19.143 | 0 | 0 | 2 | 0 | 2 |
| 80. | 172.23.19.144 | 0 | 0 | 0 | 0 | 0 |
| 81. | 172.23.19.145 | 0 | 0 | 0 | 0 | 0 |
| 82. | 172.23.19.146 | 0 | 0 | 2 | 0 | 2 |
| 83. | 172.23.19.147 | 0 | 0 | 2 | 0 | 2 |
| 84. | 172.23.19.148 | 0 | 0 | 3 | 0 | 3 |
| 85. | 172.23.19.161 | 0 | 0 | 2 | 0 | 2 |
| 86. | 172.23.19.162 | 0 | 0 | 2 | 0 | 2 |
| 87. | 172.23.19.163 | 0 | 0 | 2 | 0 | 2 |
| 88. | 172.23.19.164 | 0 | 0 | 0 | 0 | 0 |
| 89. | 172.23.19.201 | 0 | 0 | 3 | 0 | 3 |
| 90. | 172.23.19.203 | 0 | 0 | 3 | 0 | 3 |
| 91. | 172.23.19.205 | 0 | 0 | 2 | 0 | 2 |
| 92. | 172.23.19.206 | 0 | 0 | 0 | 0 | 0 |
| 93. | 172.23.19.215 | 0 | 0 | 3 | 0 | 3 |
| 94. | 172.23.19.216 | 0 | 0 | 3 | 0 | 3 |
| Summary | | 0 | 0 | 91 | 33 | 124 |

| 172.23.30.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 172.23.30.1 | 0 | 0 | 0 | 1 | 1 |
| 2. | 172.23.30.2 | 0 | 0 | 0 | 1 | 1 |
| 3. | 172.23.30.3 | 0 | 0 | 0 | 1 | 1 |
| 4. | 172.23.30.4 | 0 | 0 | 0 | 1 | 1 |
| 5. | 172.23.30.5 | 0 | 0 | 0 | 1 | 1 |
| 6. | 172.23.30.6 | 0 | 0 | 0 | 1 | 1 |
| 7. | 172.23.30.11 | 0 | 0 | 0 | 0 | 0 |
| 8. | 172.23.30.12 | 0 | 0 | 0 | 0 | 0 |
| 9. | 172.23.30.13 | 0 | 0 | 0 | 0 | 0 |
| 10. | 172.23.30.14 | 0 | 0 | 0 | 0 | 0 |
| 11. | 172.23.30.15 | 0 | 0 | 0 | 0 | 0 |
| 12. | 172.23.30.16 | 0 | 0 | 0 | 0 | 0 |
| 13. | 172.23.30.17 | 0 | 0 | 0 | 0 | 0 |
| 14. | 172.23.30.18 | 0 | 0 | 0 | 0 | 0 |
| 15. | 172.23.30.19 | 0 | 0 | 0 | 0 | 0 |
| 16. | 172.23.30.51 | 0 | 0 | 0 | 1 | 1 |
| 17. | 172.23.30.52 | 0 | 0 | 0 | 1 | 1 |
| 18. | 172.23.30.53 | 0 | 0 | 0 | 1 | 1 |
| 19. | 172.23.30.54 | 0 | 0 | 0 | 1 | 1 |
| 20. | 172.23.30.55 | 0 | 0 | 0 | 0 | 0 |
| 21. | 172.23.30.56 | 0 | 0 | 0 | 0 | 0 |
| 22. | 172.23.30.71 | 0 | 0 | 0 | 0 | 0 |
| 23. | 172.23.30.72 | 0 | 0 | 0 | 0 | 0 |
| 24. | 172.23.30.73 | 0 | 0 | 0 | 0 | 0 |
| 25. | 172.23.30.74 | 0 | 0 | 0 | 0 | 0 |
| 26. | 172.23.30.75 | 0 | 0 | 0 | 0 | 0 |
| 27. | 172.23.30.76 | 0 | 0 | 0 | 0 | 0 |
| 28. | 172.23.30.77 | 0 | 0 | 0 | 0 | 0 |
| 29. | 172.23.30.78 | 0 | 0 | 0 | 0 | 0 |
| 30. | 172.23.30.79 | 0 | 0 | 0 | 0 | 0 |
| 31. | 172.23.30.101 | 0 | 0 | 0 | 0 | 0 |
| 32. | 172.23.30.102 | 0 | 0 | 0 | 0 | 0 |
| 33. | 172.23.30.103 | 0 | 0 | 2 | 0 | 2 |
| 34. | 172.23.30.104 | 0 | 0 | 0 | 0 | 0 |
| 35. | 172.23.30.105 | 0 | 0 | 0 | 0 | 0 |
| 36. | 172.23.30.106 | 0 | 0 | 2 | 0 | 2 |
| 37. | 172.23.30.111 | 0 | 0 | 0 | 0 | 0 |
| 38. | 172.23.30.112 | 0 | 0 | 2 | 0 | 2 |
| 39. | 172.23.30.113 | 0 | 0 | 0 | 0 | 0 |
| 40. | 172.23.30.114 | 0 | 0 | 0 | 0 | 0 |
| 41. | 172.23.30.115 | 0 | 0 | 0 | 0 | 0 |
| 42. | 172.23.30.116 | 0 | 0 | 2 | 0 | 2 |
| 43. | 172.23.30.117 | 0 | 0 | 2 | 0 | 2 |
| 44. | 172.23.30.118 | 0 | 0 | 2 | 0 | 2 |
| 45. | 172.23.30.119 | 0 | 0 | 2 | 0 | 2 |
| 46. | 172.23.30.151 | 0 | 0 | 2 | 0 | 2 |
| 47. | 172.23.30.152 | 0 | 0 | 0 | 0 | 0 |
| 48. | 172.23.30.153 | 0 | 0 | 2 | 0 | 2 |
| 49. | 172.23.30.154 | 0 | 0 | 2 | 0 | 2 |
| 50. | 172.23.30.155 | 0 | 0 | 0 | 0 | 0 |
| 51. | 172.23.30.156 | 0 | 0 | 2 | 0 | 2 |
| 52. | 172.23.30.171 | 0 | 0 | 0 | 0 | 0 |
| 53. | 172.23.30.172 | 0 | 0 | 0 | 0 | 0 |
| 54. | 172.23.30.173 | 0 | 0 | 0 | 0 | 0 |
| 55. | 172.23.30.174 | 0 | 0 | 0 | 0 | 0 |
| 56. | 172.23.30.175 | 0 | 0 | 0 | 0 | 0 |
| 57. | 172.23.30.176 | 0 | 0 | 2 | 0 | 2 |
| 58. | 172.23.30.177 | 0 | 0 | 2 | 0 | 2 |
| 59. | 172.23.30.178 | 0 | 0 | 2 | 0 | 2 |
| 60. | 172.23.30.179 | 0 | 0 | 0 | 0 | 0 |
| Summary | | 0 | 0 | 28 | 10 | 38 |

| 172.23.31.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 172.23.31.1 | 0 | 0 | 0 | 0 | 0 |
| 2. | 172.23.31.2 | 0 | 0 | 0 | 0 | 0 |
| 3. | 172.23.31.5 | 0 | 0 | 0 | 1 | 1 |
| 4. | 172.23.31.6 | 0 | 0 | 0 | 1 | 1 |
| 5. | 172.23.31.11 | 0 | 0 | 0 | 0 | 0 |
| 6. | 172.23.31.12 | 0 | 0 | 0 | 0 | 0 |
| 7. | 172.23.31.13 | 0 | 0 | 0 | 0 | 0 |
| 8. | 172.23.31.14 | 0 | 0 | 0 | 0 | 0 |
| 9. | 172.23.31.15 | 0 | 0 | 0 | 0 | 0 |
| 10. | 172.23.31.16 | 0 | 0 | 0 | 0 | 0 |
| 11. | 172.23.31.17 | 0 | 0 | 0 | 0 | 0 |
| 12. | 172.23.31.18 | 0 | 0 | 0 | 0 | 0 |
| 13. | 172.23.31.19 | 0 | 0 | 0 | 0 | 0 |
| 14. | 172.23.31.51 | 0 | 0 | 0 | 1 | 1 |
| 15. | 172.23.31.52 | 0 | 0 | 0 | 1 | 1 |
| 16. | 172.23.31.55 | 0 | 0 | 0 | 1 | 1 |
| 17. | 172.23.31.56 | 0 | 0 | 0 | 1 | 1 |
| 18. | 172.23.31.57 | 0 | 0 | 0 | 1 | 1 |
| 19. | 172.23.31.58 | 0 | 0 | 0 | 0 | 0 |
| 20. | 172.23.31.59 | 0 | 0 | 0 | 0 | 0 |
| 21. | 172.23.31.60 | 0 | 0 | 0 | 1 | 1 |
| 22. | 172.23.31.61 | 0 | 0 | 0 | 0 | 0 |
| 23. | 172.23.31.62 | 0 | 0 | 0 | 0 | 0 |
| 24. | 172.23.31.63 | 0 | 0 | 0 | 0 | 0 |
| 25. | 172.23.31.64 | 0 | 0 | 0 | 0 | 0 |
| 26. | 172.23.31.65 | 0 | 0 | 0 | 0 | 0 |
| 27. | 172.23.31.66 | 0 | 0 | 0 | 0 | 0 |
| 28. | 172.23.31.67 | 0 | 0 | 0 | 0 | 0 |
| 29. | 172.23.31.68 | 0 | 0 | 0 | 0 | 0 |
| 30. | 172.23.31.69 | 0 | 0 | 0 | 0 | 0 |
| 31. | 172.23.31.101 | 0 | 0 | 2 | 0 | 2 |
| 32. | 172.23.31.102 | 0 | 0 | 2 | 0 | 2 |
| 33. | 172.23.31.105 | 0 | 0 | 2 | 0 | 2 |
| 34. | 172.23.31.106 | 0 | 0 | 2 | 0 | 2 |
| 35. | 172.23.31.111 | 0 | 0 | 2 | 0 | 2 |
| 36. | 172.23.31.112 | 0 | 0 | 2 | 0 | 2 |
| 37. | 172.23.31.113 | 0 | 0 | 0 | 0 | 0 |
| 38. | 172.23.31.114 | 0 | 0 | 2 | 0 | 2 |
| 39. | 172.23.31.115 | 0 | 0 | 2 | 0 | 2 |
| 40. | 172.23.31.116 | 0 | 0 | 2 | 0 | 2 |
| 41. | 172.23.31.117 | 0 | 0 | 0 | 0 | 0 |
| 42. | 172.23.31.118 | 0 | 0 | 2 | 0 | 2 |
| 43. | 172.23.31.119 | 0 | 0 | 2 | 0 | 2 |
| 44. | 172.23.31.151 | 0 | 0 | 2 | 0 | 2 |
| 45. | 172.23.31.152 | 0 | 0 | 2 | 0 | 2 |
| 46. | 172.23.31.155 | 0 | 0 | 2 | 0 | 2 |
| 47. | 172.23.31.156 | 0 | 0 | 2 | 0 | 2 |
| 48. | 172.23.31.157 | 0 | 0 | 2 | 0 | 2 |
| 49. | 172.23.31.158 | 0 | 0 | 2 | 0 | 2 |
| 50. | 172.23.31.159 | 0 | 0 | 2 | 0 | 2 |
| 51. | 172.23.31.160 | 0 | 0 | 2 | 0 | 2 |
| 52. | 172.23.31.161 | 0 | 0 | 0 | 0 | 0 |
| 53. | 172.23.31.162 | 0 | 0 | 2 | 0 | 2 |
| 54. | 172.23.31.163 | 0 | 0 | 2 | 0 | 2 |
| 55. | 172.23.31.164 | 0 | 0 | 2 | 0 | 2 |
| 56. | 172.23.31.165 | 0 | 0 | 2 | 0 | 2 |
| 57. | 172.23.31.166 | 0 | 0 | 2 | 0 | 2 |
| 58. | 172.23.31.167 | 0 | 0 | 2 | 0 | 2 |
| 59. | 172.23.31.168 | 0 | 0 | 2 | 0 | 2 |
| 60. | 172.23.31.169 | 0 | 0 | 2 | 0 | 2 |
| Summary | | 0 | 0 | 54 | 8 | 62 |

| 172.23.50.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 172.23.50.1 | 0 | 0 | 7 | 0 | 7 |
| 2. | 172.23.50.2 | 0 | 0 | 7 | 0 | 7 |
| 3. | 172.23.50.3 | 0 | 0 | 7 | 0 | 7 |
| 4. | 172.23.50.7 | 0 | 0 | 7 | 0 | 7 |
| 5. | 172.23.50.8 | 0 | 0 | 7 | 0 | 7 |
| 6. | 172.23.50.51 | 0 | 0 | 7 | 0 | 7 |
| 7. | 172.23.50.52 | 0 | 0 | 7 | 0 | 7 |
| 8. | 172.23.50.53 | 0 | 0 | 7 | 0 | 7 |
| 9. | 172.23.50.57 | 0 | 0 | 7 | 0 | 7 |
| 10. | 172.23.50.58 | 0 | 0 | 7 | 0 | 7 |
| 11. | 172.23.50.100 | 1 | 0 | 4 | 0 | 5 |
| 12. | 172.23.50.101 | 0 | 0 | 2 | 0 | 2 |
| 13. | 172.23.50.102 | 0 | 0 | 2 | 0 | 2 |
| 14. | 172.23.50.103 | 0 | 0 | 2 | 0 | 2 |
| 15. | 172.23.50.107 | 0 | 0 | 0 | 0 | 0 |
| 16. | 172.23.50.108 | 0 | 0 | 2 | 0 | 2 |
| 17. | 172.23.50.151 | 0 | 0 | 2 | 0 | 2 |
| 18. | 172.23.50.152 | 0 | 0 | 2 | 0 | 2 |
| 19. | 172.23.50.153 | 0 | 0 | 2 | 0 | 2 |
| 20. | 172.23.50.157 | 0 | 0 | 0 | 0 | 0 |
| 21. | 172.23.50.158 | 0 | 0 | 2 | 0 | 2 |
| Summary | | 1 | 0 | 90 | 0 | 91 |

| 172.23.70.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 172.23.70.1 | 0 | 0 | 6 | 0 | 6 |
| 2. | 172.23.70.2 | 0 | 0 | 0 | 0 | 0 |
| 3. | 172.23.70.3 | 0 | 0 | 5 | 0 | 5 |
| 4. | 172.23.70.7 | 0 | 0 | 3 | 0 | 3 |
| 5. | 172.23.70.8 | 0 | 0 | 5 | 0 | 5 |
| 6. | 172.23.70.21 | 0 | 0 | 3 | 0 | 3 |
| 7. | 172.23.70.22 | 0 | 0 | 7 | 0 | 7 |
| 8. | 172.23.70.23 | 0 | 0 | 5 | 0 | 5 |
| 9. | 172.23.70.26 | 0 | 0 | 5 | 0 | 5 |
| 10. | 172.23.70.27 | 0 | 0 | 5 | 0 | 5 |
| 11. | 172.23.70.31 | 0 | 0 | 3 | 0 | 3 |
| 12. | 172.23.70.32 | 0 | 0 | 5 | 0 | 5 |
| 13. | 172.23.70.33 | 0 | 0 | 7 | 0 | 7 |
| 14. | 172.23.70.36 | 0 | 0 | 7 | 0 | 7 |
| 15. | 172.23.70.37 | 0 | 0 | 7 | 0 | 7 |
| 16. | 172.23.70.41 | 0 | 0 | 7 | 0 | 7 |
| 17. | 172.23.70.42 | 0 | 0 | 3 | 0 | 3 |
| 18. | 172.23.70.43 | 0 | 0 | 5 | 0 | 5 |
| 19. | 172.23.70.44 | 0 | 0 | 6 | 0 | 6 |
| 20. | 172.23.70.45 | 0 | 0 | 3 | 0 | 3 |
| 21. | 172.23.70.46 | 0 | 0 | 0 | 0 | 0 |
| 22. | 172.23.70.47 | 0 | 0 | 7 | 0 | 7 |
| 23. | 172.23.70.48 | 0 | 0 | 5 | 0 | 5 |
| 24. | 172.23.70.51 | 0 | 0 | 7 | 0 | 7 |
| 25. | 172.23.70.52 | 0 | 0 | 7 | 0 | 7 |
| 26. | 172.23.70.53 | 0 | 0 | 5 | 0 | 5 |
| 27. | 172.23.70.54 | 0 | 0 | 7 | 0 | 7 |
| 28. | 172.23.70.57 | 0 | 0 | 5 | 0 | 5 |
| 29. | 172.23.70.58 | 0 | 0 | 5 | 0 | 5 |
| 30. | 172.23.70.88 | 0 | 0 | 7 | 0 | 7 |
| 31. | 172.23.70.89 | 0 | 0 | 7 | 0 | 7 |
| 32. | 172.23.70.90 | 0 | 0 | 5 | 0 | 5 |
| 33. | 172.23.70.91 | 0 | 0 | 7 | 0 | 7 |
| 34. | 172.23.70.92 | 0 | 0 | 7 | 0 | 7 |
| 35. | 172.23.70.93 | 0 | 0 | 7 | 0 | 7 |
| 36. | 172.23.70.94 | 0 | 0 | 7 | 0 | 7 |
| 37. | 172.23.70.95 | 0 | 0 | 7 | 0 | 7 |
| 38. | 172.23.70.96 | 0 | 0 | 7 | 0 | 7 |
| 39. | 172.23.70.100 | 0 | 0 | 2 | 0 | 2 |
| 40. | 172.23.70.101 | 0 | 0 | 0 | 0 | 0 |
| 41. | 172.23.70.102 | 0 | 0 | 2 | 0 | 2 |
| 42. | 172.23.70.103 | 0 | 0 | 2 | 0 | 2 |
| 43. | 172.23.70.107 | 0 | 0 | 0 | 0 | 0 |
| 44. | 172.23.70.108 | 0 | 0 | 0 | 0 | 0 |
| 45. | 172.23.70.121 | 0 | 0 | 0 | 0 | 0 |
| 46. | 172.23.70.122 | 0 | 0 | 2 | 0 | 2 |
| 47. | 172.23.70.123 | 0 | 0 | 0 | 0 | 0 |
| 48. | 172.23.70.126 | 0 | 0 | 2 | 0 | 2 |
| 49. | 172.23.70.127 | 0 | 0 | 2 | 0 | 2 |
| 50. | 172.23.70.131 | 0 | 0 | 2 | 0 | 2 |
| 51. | 172.23.70.132 | 0 | 0 | 2 | 0 | 2 |
| 52. | 172.23.70.133 | 0 | 0 | 0 | 0 | 0 |
| 53. | 172.23.70.136 | 0 | 0 | 2 | 0 | 2 |
| 54. | 172.23.70.137 | 0 | 0 | 2 | 0 | 2 |
| 55. | 172.23.70.141 | 0 | 0 | 2 | 0 | 2 |
| 56. | 172.23.70.142 | 0 | 0 | 0 | 0 | 0 |
| 57. | 172.23.70.143 | 0 | 0 | 2 | 0 | 2 |
| 58. | 172.23.70.144 | 0 | 0 | 2 | 0 | 2 |
| 59. | 172.23.70.145 | 0 | 0 | 2 | 0 | 2 |
| 60. | 172.23.70.146 | 0 | 0 | 0 | 0 | 0 |
| 61. | 172.23.70.147 | 0 | 0 | 0 | 0 | 0 |
| 62. | 172.23.70.148 | 0 | 0 | 2 | 0 | 2 |
| 63. | 172.23.70.150 | 0 | 0 | 3 | 0 | 3 |
| 64. | 172.23.70.151 | 0 | 0 | 0 | 0 | 0 |
| 65. | 172.23.70.152 | 0 | 0 | 2 | 0 | 2 |
| 66. | 172.23.70.153 | 0 | 0 | 0 | 0 | 0 |
| 67. | 172.23.70.154 | 0 | 0 | 0 | 0 | 0 |
| 68. | 172.23.70.157 | 0 | 0 | 2 | 0 | 2 |
| 69. | 172.23.70.158 | 0 | 0 | 2 | 0 | 2 |
| 70. | 172.23.70.180 | 1 | 0 | 4 | 0 | 5 |
| 71. | 172.23.70.188 | 0 | 0 | 2 | 0 | 2 |
| 72. | 172.23.70.189 | 0 | 0 | 2 | 0 | 2 |
| 73. | 172.23.70.190 | 0 | 0 | 2 | 0 | 2 |
| 74. | 172.23.70.191 | 0 | 0 | 2 | 0 | 2 |
| 75. | 172.23.70.192 | 0 | 0 | 0 | 0 | 0 |
| 76. | 172.23.70.193 | 0 | 0 | 2 | 0 | 2 |
| 77. | 172.23.70.194 | 0 | 0 | 2 | 0 | 2 |
| 78. | 172.23.70.195 | 0 | 0 | 2 | 0 | 2 |
| 79. | 172.23.70.196 | 0 | 0 | 0 | 0 | 0 |
| 80. | 172.23.70.201 | 0 | 0 | 2 | 0 | 2 |
| 81. | 172.23.70.202 | 0 | 0 | 2 | 0 | 2 |
| 82. | 172.23.70.203 | 0 | 0 | 2 | 0 | 2 |
| 83. | 172.23.70.205 | 0 | 0 | 2 | 0 | 2 |
| 84. | 172.23.70.206 | 0 | 0 | 2 | 0 | 2 |
| 85. | 172.23.70.207 | 0 | 0 | 0 | 0 | 0 |
| 86. | 172.23.70.208 | 0 | 0 | 0 | 0 | 0 |
| Summary | | 1 | 0 | 273 | 0 | 274 |

| 172.23.80.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 172.23.80.1 | 0 | 0 | 7 | 0 | 7 |
| 2. | 172.23.80.2 | 0 | 0 | 7 | 0 | 7 |
| 3. | 172.23.80.3 | 0 | 0 | 7 | 0 | 7 |
| 4. | 172.23.80.7 | 0 | 0 | 7 | 0 | 7 |
| 5. | 172.23.80.8 | 0 | 0 | 7 | 0 | 7 |
| 6. | 172.23.80.11 | 0 | 0 | 7 | 0 | 7 |
| 7. | 172.23.80.12 | 0 | 0 | 7 | 0 | 7 |
| 8. | 172.23.80.13 | 0 | 0 | 7 | 0 | 7 |
| 9. | 172.23.80.14 | 0 | 0 | 7 | 0 | 7 |
| 10. | 172.23.80.31 | 0 | 0 | 7 | 0 | 7 |
| 11. | 172.23.80.32 | 0 | 0 | 7 | 0 | 7 |
| 12. | 172.23.80.33 | 0 | 0 | 7 | 0 | 7 |
| 13. | 172.23.80.34 | 0 | 0 | 7 | 0 | 7 |
| 14. | 172.23.80.35 | 0 | 0 | 7 | 0 | 7 |
| 15. | 172.23.80.36 | 0 | 0 | 7 | 0 | 7 |
| 16. | 172.23.80.37 | 0 | 0 | 7 | 0 | 7 |
| 17. | 172.23.80.38 | 0 | 0 | 7 | 0 | 7 |
| 18. | 172.23.80.39 | 0 | 0 | 7 | 0 | 7 |
| 19. | 172.23.80.51 | 0 | 0 | 7 | 0 | 7 |
| 20. | 172.23.80.52 | 0 | 0 | 7 | 0 | 7 |
| 21. | 172.23.80.53 | 0 | 0 | 7 | 0 | 7 |
| 22. | 172.23.80.57 | 0 | 0 | 7 | 0 | 7 |
| 23. | 172.23.80.58 | 0 | 0 | 7 | 0 | 7 |
| 24. | 172.23.80.71 | 0 | 0 | 7 | 0 | 7 |
| 25. | 172.23.80.72 | 0 | 0 | 7 | 0 | 7 |
| 26. | 172.23.80.73 | 0 | 0 | 7 | 0 | 7 |
| 27. | 172.23.80.74 | 0 | 0 | 7 | 0 | 7 |
| 28. | 172.23.80.81 | 0 | 0 | 7 | 0 | 7 |
| 29. | 172.23.80.82 | 0 | 0 | 7 | 0 | 7 |
| 30. | 172.23.80.83 | 0 | 0 | 7 | 0 | 7 |
| 31. | 172.23.80.84 | 0 | 0 | 7 | 0 | 7 |
| 32. | 172.23.80.85 | 0 | 0 | 7 | 0 | 7 |
| 33. | 172.23.80.86 | 0 | 0 | 7 | 0 | 7 |
| 34. | 172.23.80.87 | 0 | 0 | 7 | 0 | 7 |
| 35. | 172.23.80.88 | 0 | 0 | 7 | 0 | 7 |
| 36. | 172.23.80.89 | 0 | 0 | 7 | 0 | 7 |
| 37. | 172.23.80.100 | 0 | 0 | 4 | 0 | 4 |
| 38. | 172.23.80.101 | 0 | 0 | 2 | 0 | 2 |
| 39. | 172.23.80.102 | 0 | 0 | 2 | 0 | 2 |
| 40. | 172.23.80.103 | 0 | 0 | 2 | 0 | 2 |
| 41. | 172.23.80.107 | 0 | 0 | 2 | 0 | 2 |
| 42. | 172.23.80.108 | 0 | 0 | 2 | 0 | 2 |
| 43. | 172.23.80.111 | 0 | 0 | 2 | 0 | 2 |
| 44. | 172.23.80.112 | 0 | 0 | 2 | 0 | 2 |
| 45. | 172.23.80.113 | 0 | 0 | 2 | 0 | 2 |
| 46. | 172.23.80.114 | 0 | 0 | 2 | 0 | 2 |
| 47. | 172.23.80.131 | 0 | 0 | 2 | 0 | 2 |
| 48. | 172.23.80.132 | 0 | 0 | 2 | 0 | 2 |
| 49. | 172.23.80.133 | 0 | 0 | 2 | 0 | 2 |
| 50. | 172.23.80.134 | 0 | 0 | 2 | 0 | 2 |
| 51. | 172.23.80.135 | 0 | 0 | 2 | 0 | 2 |
| 52. | 172.23.80.136 | 0 | 0 | 0 | 0 | 0 |
| 53. | 172.23.80.137 | 0 | 0 | 2 | 0 | 2 |
| 54. | 172.23.80.138 | 0 | 0 | 2 | 0 | 2 |
| 55. | 172.23.80.139 | 0 | 0 | 2 | 0 | 2 |
| 56. | 172.23.80.150 | 1 | 0 | 4 | 0 | 5 |
| 57. | 172.23.80.151 | 0 | 0 | 2 | 0 | 2 |
| 58. | 172.23.80.152 | 0 | 0 | 2 | 0 | 2 |
| 59. | 172.23.80.153 | 0 | 0 | 2 | 0 | 2 |
| 60. | 172.23.80.157 | 0 | 0 | 2 | 0 | 2 |
| 61. | 172.23.80.158 | 0 | 0 | 2 | 0 | 2 |
| 62. | 172.23.80.171 | 0 | 0 | 2 | 0 | 2 |
| 63. | 172.23.80.172 | 0 | 0 | 2 | 0 | 2 |
| 64. | 172.23.80.173 | 0 | 0 | 2 | 0 | 2 |
| 65. | 172.23.80.174 | 0 | 0 | 2 | 0 | 2 |
| 66. | 172.23.80.180 | 1 | 0 | 4 | 0 | 5 |
| 67. | 172.23.80.181 | 0 | 0 | 2 | 0 | 2 |
| 68. | 172.23.80.182 | 0 | 0 | 2 | 0 | 2 |
| 69. | 172.23.80.183 | 0 | 0 | 2 | 0 | 2 |
| 70. | 172.23.80.184 | 0 | 0 | 2 | 0 | 2 |
| 71. | 172.23.80.185 | 0 | 0 | 2 | 0 | 2 |
| 72. | 172.23.80.186 | 0 | 0 | 2 | 0 | 2 |
| 73. | 172.23.80.187 | 0 | 0 | 2 | 0 | 2 |
| 74. | 172.23.80.188 | 0 | 0 | 2 | 0 | 2 |
| 75. | 172.23.80.189 | 0 | 0 | 2 | 0 | 2 |
| 76. | 172.23.80.201 | 0 | 0 | 2 | 0 | 2 |
| 77. | 172.23.80.202 | 0 | 0 | 2 | 0 | 2 |
| 78. | 172.23.80.203 | 0 | 0 | 2 | 0 | 2 |
| 79. | 172.23.80.204 | 0 | 0 | 2 | 0 | 2 |
| 80. | 172.23.80.205 | 0 | 0 | 2 | 0 | 2 |
| 81. | 172.23.80.206 | 0 | 0 | 2 | 0 | 2 |
| Summary | | 2 | 0 | 346 | 0 | 348 |

| 172.23.90.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 172.23.90.1 | 0 | 0 | 6 | 0 | 6 |
| 2. | 172.23.90.2 | 0 | 0 | 6 | 0 | 6 |
| 3. | 172.23.90.3 | 1 | 1 | 7 | 0 | 9 |
| 4. | 172.23.90.6 | 0 | 0 | 7 | 0 | 7 |
| 5. | 172.23.90.7 | 0 | 0 | 6 | 0 | 6 |
| 6. | 172.23.90.8 | 0 | 0 | 7 | 0 | 7 |
| 7. | 172.23.90.10 | 0 | 0 | 6 | 0 | 6 |
| 8. | 172.23.90.11 | 1 | 1 | 7 | 0 | 9 |
| 9. | 172.23.90.12 | 0 | 0 | 5 | 0 | 5 |
| 10. | 172.23.90.13 | 0 | 0 | 7 | 0 | 7 |
| 11. | 172.23.90.21 | 0 | 0 | 7 | 0 | 7 |
| 12. | 172.23.90.22 | 0 | 0 | 7 | 0 | 7 |
| 13. | 172.23.90.23 | 0 | 0 | 7 | 0 | 7 |
| 14. | 172.23.90.24 | 0 | 0 | 7 | 0 | 7 |
| 15. | 172.23.90.25 | 0 | 0 | 7 | 0 | 7 |
| 16. | 172.23.90.26 | 0 | 0 | 7 | 0 | 7 |
| 17. | 172.23.90.27 | 0 | 0 | 7 | 0 | 7 |
| 18. | 172.23.90.28 | 0 | 0 | 7 | 0 | 7 |
| 19. | 172.23.90.29 | 0 | 0 | 7 | 0 | 7 |
| 20. | 172.23.90.51 | 1 | 1 | 7 | 0 | 9 |
| 21. | 172.23.90.52 | 1 | 1 | 7 | 0 | 9 |
| 22. | 172.23.90.53 | 1 | 1 | 7 | 0 | 9 |
| 23. | 172.23.90.54 | 0 | 0 | 7 | 0 | 7 |
| 24. | 172.23.90.55 | 0 | 0 | 7 | 0 | 7 |
| 25. | 172.23.90.56 | 0 | 0 | 7 | 0 | 7 |
| 26. | 172.23.90.60 | 1 | 1 | 7 | 0 | 9 |
| 27. | 172.23.90.61 | 0 | 0 | 6 | 0 | 6 |
| 28. | 172.23.90.62 | 0 | 0 | 7 | 0 | 7 |
| 29. | 172.23.90.63 | 0 | 0 | 7 | 0 | 7 |
| 30. | 172.23.90.91 | 0 | 0 | 7 | 0 | 7 |
| 31. | 172.23.90.92 | 0 | 0 | 7 | 0 | 7 |
| 32. | 172.23.90.93 | 0 | 0 | 7 | 0 | 7 |
| 33. | 172.23.90.94 | 0 | 0 | 7 | 0 | 7 |
| 34. | 172.23.90.95 | 0 | 0 | 7 | 0 | 7 |
| 35. | 172.23.90.100 | 0 | 0 | 4 | 0 | 4 |
| 36. | 172.23.90.101 | 0 | 0 | 2 | 0 | 2 |
| 37. | 172.23.90.102 | 0 | 0 | 2 | 0 | 2 |
| 38. | 172.23.90.103 | 0 | 0 | 2 | 0 | 2 |
| 39. | 172.23.90.106 | 0 | 0 | 2 | 0 | 2 |
| 40. | 172.23.90.107 | 0 | 0 | 2 | 0 | 2 |
| 41. | 172.23.90.108 | 0 | 0 | 2 | 0 | 2 |
| 42. | 172.23.90.110 | 0 | 0 | 2 | 0 | 2 |
| 43. | 172.23.90.111 | 0 | 0 | 2 | 0 | 2 |
| 44. | 172.23.90.112 | 0 | 0 | 2 | 0 | 2 |
| 45. | 172.23.90.113 | 0 | 0 | 2 | 0 | 2 |
| 46. | 172.23.90.121 | 0 | 0 | 2 | 0 | 2 |
| 47. | 172.23.90.122 | 0 | 0 | 2 | 0 | 2 |
| 48. | 172.23.90.123 | 0 | 0 | 2 | 0 | 2 |
| 49. | 172.23.90.124 | 0 | 0 | 2 | 0 | 2 |
| 50. | 172.23.90.125 | 0 | 0 | 2 | 0 | 2 |
| 51. | 172.23.90.126 | 0 | 0 | 2 | 0 | 2 |
| 52. | 172.23.90.127 | 0 | 0 | 2 | 0 | 2 |
| 53. | 172.23.90.128 | 0 | 0 | 0 | 0 | 0 |
| 54. | 172.23.90.129 | 0 | 0 | 2 | 0 | 2 |
| 55. | 172.23.90.150 | 0 | 0 | 4 | 0 | 4 |
| 56. | 172.23.90.151 | 0 | 0 | 2 | 0 | 2 |
| 57. | 172.23.90.152 | 0 | 0 | 2 | 0 | 2 |
| 58. | 172.23.90.153 | 0 | 0 | 2 | 0 | 2 |
| 59. | 172.23.90.154 | 0 | 0 | 2 | 0 | 2 |
| 60. | 172.23.90.155 | 0 | 0 | 2 | 0 | 2 |
| 61. | 172.23.90.156 | 0 | 0 | 2 | 0 | 2 |
| 62. | 172.23.90.160 | 0 | 0 | 2 | 0 | 2 |
| 63. | 172.23.90.161 | 0 | 0 | 2 | 0 | 2 |
| 64. | 172.23.90.162 | 0 | 0 | 2 | 0 | 2 |
| 65. | 172.23.90.163 | 0 | 0 | 2 | 0 | 2 |
| 66. | 172.23.90.191 | 0 | 0 | 0 | 0 | 0 |
| 67. | 172.23.90.192 | 0 | 0 | 2 | 0 | 2 |
| 68. | 172.23.90.193 | 0 | 0 | 2 | 0 | 2 |
| 69. | 172.23.90.194 | 0 | 0 | 2 | 0 | 2 |
| 70. | 172.23.90.195 | 0 | 0 | 2 | 0 | 2 |
| 71. | 172.23.90.201 | 0 | 0 | 0 | 0 | 0 |
| 72. | 172.23.90.202 | 0 | 0 | 0 | 0 | 0 |
| 73. | 172.23.90.203 | 0 | 0 | 2 | 0 | 2 |
| 74. | 172.23.90.204 | 0 | 0 | 2 | 0 | 2 |
| 75. | 172.23.90.205 | 0 | 0 | 0 | 0 | 0 |
| 76. | 172.23.90.206 | 0 | 0 | 2 | 0 | 2 |
| Summary | | 6 | 6 | 309 | 0 | 321 |

| 172.24.20.0 | | Risk Level | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| No. | IP | Critical | High | Medium | Low | Summary |
| 1. | 172.24.20.1 | 0 | 0 | 0 | 0 | 0 |
| 2. | 172.24.20.2 | 0 | 0 | 0 | 0 | 0 |
| 3. | 172.24.20.3 | 0 | 0 | 0 | 0 | 0 |
| 4. | 172.24.20.4 | 0 | 0 | 0 | 0 | 0 |
| 5. | 172.24.20.5 | 0 | 0 | 0 | 0 | 0 |
| 6. | 172.24.20.6 | 0 | 0 | 0 | 0 | 0 |
| 7. | 172.24.20.7 | 0 | 0 | 0 | 0 | 0 |
| 8. | 172.24.20.8 | 0 | 0 | 0 | 0 | 0 |
| 9. | 172.24.20.9 | 0 | 0 | 0 | 0 | 0 |
| 10. | 172.24.20.51 | 0 | 0 | 0 | 0 | 0 |
| 11. | 172.24.20.52 | 0 | 0 | 0 | 0 | 0 |
| 12. | 172.24.20.53 | 0 | 0 | 0 | 0 | 0 |
| 13. | 172.24.20.54 | 0 | 0 | 0 | 0 | 0 |
| 14. | 172.24.20.55 | 0 | 0 | 0 | 0 | 0 |
| 15. | 172.24.20.56 | 0 | 0 | 0 | 0 | 0 |
| 16. | 172.24.20.57 | 0 | 0 | 0 | 0 | 0 |
| 17. | 172.24.20.58 | 0 | 0 | 0 | 0 | 0 |
| 18. | 172.24.20.59 | 0 | 0 | 0 | 0 | 0 |
| 19. | 172.24.20.101 | 0 | 0 | 2 | 0 | 2 |
| 20. | 172.24.20.102 | 0 | 0 | 2 | 0 | 2 |
| 21. | 172.24.20.103 | 0 | 0 | 2 | 0 | 2 |
| 22. | 172.24.20.104 | 0 | 0 | 2 | 0 | 2 |
| 23. | 172.24.20.105 | 0 | 0 | 2 | 0 | 2 |
| 24. | 172.24.20.106 | 0 | 0 | 2 | 0 | 2 |
| 25. | 172.24.20.107 | 0 | 0 | 2 | 0 | 2 |
| 26. | 172.24.20.108 | 0 | 0 | 2 | 0 | 2 |
| 27. | 172.24.20.109 | 0 | 0 | 2 | 0 | 2 |
| 28. | 172.24.20.151 | 0 | 0 | 2 | 0 | 2 |
| 29. | 172.24.20.152 | 0 | 0 | 2 | 0 | 2 |
| 30. | 172.24.20.153 | 0 | 0 | 2 | 0 | 2 |
| 31. | 172.24.20.154 | 0 | 0 | 2 | 0 | 2 |
| 32. | 172.24.20.155 | 0 | 0 | 2 | 0 | 2 |
| 33. | 172.24.20.156 | 0 | 0 | 2 | 0 | 2 |
| 34. | 172.24.20.157 | 0 | 0 | 2 | 0 | 2 |
| 35. | 172.24.20.158 | 0 | 0 | 2 | 0 | 2 |
| 36. | 172.24.20.159 | 0 | 0 | 2 | 0 | 2 |
| 37. | 172.24.20.201 | 0 | 0 | 2 | 0 | 2 |
| 38. | 172.24.20.202 | 0 | 0 | 2 | 0 | 2 |
| Summary | | 0 | 0 | 40 | 0 | 40 |



**ตารางที่ 4** แสดงตารางแสดงผลช่องโหว่ Nutanix Cloud