**{{ service }}**

**{{ service }}**

{{ vendor }} was engaged by {{ client }} to conduct a {{ service\_type }} Box {{ service }} activity for the given scope. The aim of this assessment was to identify security issues in the {{ service\_scope }} that in turn could negatively affect {{ client }} business or reputation if they led to the compromise or abuse of systems.

This testing was conducted remotely from **{{ start\_date }}** to **{{ end\_date }}** by {{ authora }}, under the guidance of Steve Wozniak.

|  |  |
| --- | --- |
| **Synopsis:** | This document defines the vulnerabilities that were identified for {{ service\_detailed\_scope }} – {{ service }} engagement, as part of the service requested by the Infrastructure Owner or their representative. |
| **Status:** | Draft |
| **Author:** | {{ authorc }} |
| **Version:** | 0.1 |
| **Reviewer** | Steve Jobs, Bill Gates |
| **Date** | {{ date }} |

**Document Control Information**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Status** | **Authors** |
| 0.1 | {{ date }} | Initial Draft | {{ author1 }}  {{ author2 }} |
| 0.2 | 19-11-1958 | Document assurance One | Bill Gates |
| 0.4 | 19-11-1976 | Document assurance Two | Steve Jobs |
| 1.0 | 19-11-2019 | Final | Ada Lovelace |

**Table of Contents**

[1. Executive Summary 4](#_Toc80292021)

[1.1 Table of Findings Summary 5](#_Toc80292022)

[2. Detailed Findings 6](#_Toc80292026)

# Executive Summary

Penetration testing was performed on the {{ client }}'s environment by the {{ vendor }}'s Penetration Testing team. The testing activity took place between **{{ start\_date }}** and **{{ end\_date }}** from the **{{ vpn }} VPN** provided by {{ client }}.

Brief description of the {{ client }} scope:

{{ client }} assets comprises of 1000+ Routers, switches and other types of network devices along with 10+ different types of servers.

The result of the engagement indicates that the {{ client }} {{ service }} has room for improvements.

During the assessment **{{ risk\_count }}** issues were found.

**{{ top1\_title }} Risk(s)**

The {{ top1 }}-risk findings are attributed to the following vulnerabilities:

|  |
| --- |
| {%tr for item in exec\_top1 %} |
| * ***{{ item.title }}* –** {{ item.description }} |
| {%tr endfor %} |

**{{ top2\_title }} Risk(s)**

The {{ top2 }}-risk findings are attributed to the following vulnerabilities:

|  |
| --- |
| {%tr for item in exec\_top2 %} |
| * ***{{ item.title }}* –** {{ item.description }} |
| {%tr endfor %} |

{{ vendor }} recommends that the {{ client }} Assets with the issue highlighted in this report in an effort to maintain security best practice, focusing on the critical and high-risk issues and resolving the medium issues to further strengthen the security posture.

## Table of Findings Summary

|  |  |  |
| --- | --- | --- |
| Ref. | *Finding* | Risk |
| {%tr for item in table\_contents %} | | |
| 3.{{ item.index }} | ***{{ item.title }}***  {{ item.description }} | {% cellbg item.bgcolor %}{{r item.risk }} |
| {%tr endfor %} | | |



# Detailed Findings

Below are the detailed descriptions of security risks that were identified during the review.



{% for vd in vuln %}

## {{ vd.title }}

|  |  |
| --- | --- |
| **Risk** | {{r vd.risk }}{% cellbg vd.bgcolor %} |

|  |  |
| --- | --- |
| **Impact** | {{ vd.impact }} |
| **Likelihood** | {{ vd.likelihood }} |

### Description of Finding

{{ vd.description }}

### POC

The screenshot(s) below show the {{ vd.title }}. {{ vd.imp }}

{% for p in vd.image %}

{{ p.image }}

Figure 3.1-1: {{ p.desc }}

{% endfor %}

### Remediation

{{ vd.recommendation }}

### References and additional information

* {{ vd.info }}

{% endfor %}