POL00337568

NETITUDE
AN LRQA COMPANY

Penetration Testing Technical Report

Prepared For: POST OFFICE
TARGET: COUNTER TRAINING OFFICE
AUTHOR: JORDAN WILLIAMS
Date: 21 November 2022
Version: 1.0

Confidential Security Document

POL00337568

Contents

POL00337568

1 Document Distribution List

Nettitude	Name	Title
	Jordan Williams	Managing Principal Security Consultant
	Dalton Wright	Quality Assurance
	Tom Jordan	Account Manager

Post Office	Name	Title
	Mark J Cunningham	Security Risk Manager
	Julian Higgs	Security Assurance and Governance Specialist
	Khushtar Hosenie	Risk, Security & Data Governance Manager

2 Revision History

Version	Issue Date	Issued by	Comments
0.1	21 November 2022	Jordan Williams	Initial Draft
0.2	29 November 2022	Dalton Wright	Quality Assurance
1.0	30 November 2022	Jordan Williams	Final version

POL00337568

3 Engagement Particulars

Background

This report serves as technical documentation for the recent penetration test performed for Post Office by Nettitude. For a high-level assessment of the tested environment, please refer to the accompanying management report.

Engagement Activities and Rules

Nettitude performed testing over a three-day period, 16 November to 18 November 2022. All testing originated from the Counter Training Office Post Office LTD located at Stanway House in Bristol. Nettitude adhered to the following rules.

- Social engineering was not permitted.
- Denial of Service (DoS) testing was not permitted.

Scope

Post Office tasked Nettitude to perform a black-box security assessment of the thick client application running on six kiosk systems detailed in the following table:

Component	Description
h90002300101.euc.postoffice.co.uk	10.101.69.1
h90002300102.euc.postoffice.co.uk	10.101.69.2
h90002300103.euc.postoffice.co.uk	10.101.69.3
h90002300104.euc.postoffice.co.uk	10.101.69.4
h90002300105.euc.postoffice.co.uk	10.101.69.5
h90002300106.euc.postoffice.co.uk	10.101.69.6

POL00337568

User Accounts

Nettitude made use of the following accounts to ensure that breadth of testing, as well as user related testing, was achieved:

Username	Application	Role
MMA456	Kiosk Login	Manager
CMA456	Kiosk Login	Operator

Testing Windows Observations and Constraints

The time frame provisioned for the completion of this engagement was adequate. No constraints were encountered during the engagement.

Findings Summary

Nettitude identified a total number of zero findings during the engagement. The following table shows the categorisation by severity:

0 Critical	0 High	0 Medium	0 Low	0 Info.

POL00337568

4 Analysis

During the recent penetration test that was performed against the Kiosk systems, no security vulnerabilities were identified.

Nettitude tried a number of techniques to gain access to the kiosks including performing a comprehensive port scan of all UDP and TCP ports and found some services were listening but were unable to gain access from the network to the devices in the time available. Nettitude tried a number of other methods to gain access including booting the device from an alternative source, HID attacks, and disrupting network communication to force errors without success.

By connecting a device to the network and analysing network traffic it was possible to identify the IP addresses and the FQDN of the kiosks, however, it was not possible to intercept network traffic used by the application or gain access to the ports that were identified as open on the kiosk devices.

POL00337568

5 Appendix

5.1 Vulnerability Severity Methodology

We use CVSS (Common Vulnerability Scoring System) version 3.1 to determine the severity of vulnerabilities we report. This is a widely used system which allows us to report in a consistent and actionable manner. The score ranges from 0 – 10, with higher numbers representing higher severity vulnerabilities.

Multiple factors contribute to the final CVSS score of each vulnerability. We determine a series of exploitability and impact metrics, which combine to create a base score. Depending on the level of information we have about the vulnerability and the environment it exists in, we may opt to apply some modifiers to that base score, leading to an altered final score.

The following table shows how each quantitative score is associated with a qualitative rating ranging from critical down to informational.

Severity Rating	CVSS Score	Typical Vulnerability Characteristics
CRITICAL	9.0 – 10.0	Exploitation is likely to be easy and repeatable. It is also likely to result in significant system access. There is potential for significant business impact.
HIGH	7.0 – 8.9	Exploitation is likely to be difficult and require specific user interactions or attack timing. Following exploitation, elevated system access is likely. Business impact is likely to be meaningful.
MEDIUM	4.0 – 6.9	Exploitation is difficult due for reasons such as complexity, location requirements, specific user interactions, etc. Successful exploitation is likely to lead to normal or limited system access. Business impact is likely to be low.
LOW	0.1 – 3.9	Exploitation is unlikely and resultant system access is low. Business impact is negligible. This may be more useful in tandem with one or more other vulnerabilities rather than a standalone one.

POL00337568

INFORMATIONAL	0.0	No vulnerability exists, but this is still a noteworthy finding. This may have the potential to evolve a vulnerability in future. It may represent an opportunity for improvement.

CVSS scores are calculated based on one or more of the following three metric groups: base metrics, temporal metrics, and environmental metrics. These are described in more detail below.

5.1.1 Base Metrics

The base score represents the intrinsic characteristics of each vulnerability, which remain the same over time and across all environments. The base score is comprised broadly of two metrics; the exploitability of a vulnerability and the impact it may have.

The exploitability elements reflect the ease with which the vulnerability can be exploited. Not all vulnerabilities are equally exploitable. For example, some may require specific user interactions or attack positioning, while others may be exploitable from anywhere in the world with no dependencies. The impact elements describe the immediate consequences of successful exploitation, in terms of confidentiality, integrity, and availability.

5.1.2 Temporal Metrics

The temporal metrics modify the severity of each vulnerability based on factors that change over time, such as the availability and maturity of exploit code, software patches, etc. Temporal metrics are included in our CVSS calculation when we have sufficient information to include them.

5.1.3 Environmental Metrics

Environmental Metrics modify the base score based on factors which are unique to the relevant environment, for example the existence of mitigating factors and the risk requirements of the environment. Environmental metrics are rarely included in our CVSS calculations due to insufficient information about these factors in most engagements.

5.2 Penetration Testing Methodology

Nettitude has a series of approaches for conducting Penetration Tests.

5.2.1 Black Box Testing

In a Black Box test, the client does not provide Nettitude with any information about their infrastructure. For internal tests the customer may provide no more than a network point for the tester to connect in to. For external tests, this may simply be a URL or even just the company name that is in scope for assessment.

POL00337568

Nettitude is tasked with testing the environment as if they were an attacker with no information about the infrastructure or application logic that they are testing. Black Box tests tend to take longer to commission than White Box tests and may identify less exposures and vulnerabilities than those of White Box tests.

5.2.2 White Box Testing

In a White Box test, clients provide Nettitude with information about the applications and infrastructure prior to the commencement of the testing engagement. Usernames and Passwords are provided to Nettitude's testing team as part of the engagement, and the client may provide Nettitude's consultants with access to source code. In this type of testing engagement, Nettitude works closely with the client to perform the assessment. These types of tests tend to gain deeper understanding of the application and infrastructure logic, and may generate highly comprehensive test results.

5.2.3 Grey Box Testing

A Grey Box test is a blend of Black Box testing techniques and White Box testing techniques. In Grey Box testing, clients provide Nettitude with snippets of information to help with the testing procedures. This results in a highly focused test.

POL00337568

Nettitude Penetration Testing Services

www.nettitude.com/penetration-testing/

CREST VA PEN TEST STAR STAR CSIR SOC

CBEST PCI PCI CYBER ESSENTIALS

NETTITUDE
AN LRQA COMPANY

UK Head Office
Jephson Court, Tancred Close, Leamington Spa, CV31 3RZ

Americas
50 Broad Street, Suite 403, New York, NY 10004

Asia Pacific
18 Cross Street, #02-101, Suite S2039, Singapore 048423

Europe
Leof. Siggrou 348
Kallithea, Athens, 176 74
GRO

Follow Us

solutions GRO
www.nettitude.com