Metier Desktop Application Penetration Testing– Report

Summary:	This document provides the results of the Desktop Application Penetration Testing of Metier Application. The engagement was performed by 8FoldGovernance and the findings identified are outlined in this document.

Status:	Final Report
Author:	Ivelina Ivanova / Giannis Kostakis
Date:	03/09/24
Version:	2.1

DOCUMENT CONTROL

Client Confidentiality

This document contains Client Confidential information and may not be discussed, disclosed, or copied to any third party without prior written permission from Metier.

Document Version Control			
Version No.	Issue Date	Tester	Change Description
0.1	29/07/24	Ivelina Ivanova	Initial Technical Report
1.0	02/08/24	Giannis Kostakis	Draft Report Release
2.0	23/08/24	Giannis Kostakis	Updated Report Release
2.1	03/09/24	Giannis Kostakis	Final Report Release

Document Distribution List			
Name	Job Title	Email	Telephone Number
Ivelina Ivanova	Security Analyst	Ivelina@8foldgovernance.com	+44 7440704065
Giannis Kostakis	Security Director	giannis@8foldgovernance.com	+44 7463239665

8fold GOVERNANCE

TABLE OF CONTENTS

1. Executive Summary

The purpose of this document is to present the security findings related to the Desktop Application Penetration Testing conducted by 8FoldGovernance and Leo CybSec, a CREST-Certified Company. The assessment was performed from 29/07/24 until 02/08/24 and was authorised by the Metier Management Team. Five working days were assigned in total for testing and reporting. An updated report was released on 03/09/24 after reviewing findings and mitigations with Metier team.

1.1. Scope of Testing

8FoldGovernace conducted the Grey Box Penetration Testing using automated and manual inspection techniques, based on a number of well-recognized security best practices and tools.

The applications within the scope of this test are listed below:

- CALL-CONNECT GP

The following user roles were used for the authenticated part of the testing:

Username	Role
Ivelina	User

Testing was conducted utilizing a standalone instance of CCGP components installed on the tester's laptop, which included;

- Installing SQL server 2019
- SQL Studio Manager
- Restoring a dummy database of patients and demographics, to the SQL instance.
- The suite of local PC applications (.exe's) and configuration files that compose Call Connect GP – these can be installed and run from any folder on the PC.
- A series of shortcuts – these launch Call Connect GP in an identical way to that which the CTI software for the telephone system would do so – allowing

the testing simulating incoming answered phone calls and testing functionality.

- An instance of SystmOne – Metier have their own instance of S1 for development and testing purposes – having a live Clinical System allowed testing of the interaction between CCGP and the Clinical System.

This installation also allowed the tester to see the steps included in setting up the solution and its components.

Clinical System Integration

The test setup included a live login to Metier's instance of TPP SystemOne Clinical System. The basic interaction with the clinical system was tested – this requires the clinical system instance to be running (hence appearing in the logs) and the user to already be logged into the clinical system by their normal methods (NHS Smartcard or username and password) with the clinical system in such as state as to allow a patient search.

Please see 8Fold Governance's DCB0129 Report and documentation for more details.

Testing was mainly focused on the following requirements:

- OWASP TOP 10
- DTAC Security Requirements

1.2. Limitations and Caveats

No limitations appeared during the testing window.

1.3. Conclusion

The table below summarises the final findings identified during the testing window and the process of changes to software and mitigations of identified risks.:

Severity	# of Findings Identified
Critical	-
High	-
Medium	-
Low 1	2
Informational	1
Total	3

There were no Critical or High security findings identified, and this test confirms that Metier Desktop Application meets the respective DTAC requirements.

1.4. Identified Good Practices

In light of the findings uncovered during the pentesting, it is noteworthy to highlight good practices which significantly enhance the overall security. These practices include:

1. **Secure Handling of SQL:**

   The assessed system demonstrated robust security measures against SQL injection attacks.

2. **Port filtering for SQL Server:**

   SQL is configured not to use dynamic ports but standard TCP and UDP SQL ports. Those ports are allowed only to be used through NHS Firewalls. The default SQL Server ports 1433 & 1434, used by the application, is configured to be filtered in the SQL Server Configuration Manager.

3. **Collaborative Team Involvement:**

   The application team actively participated in the project, providing the necessary support to successfully replicate the production environment, troubleshoot issues, and complete the security assessment.

1.5. The Process Steps To Reach The Final Report and Future Recommendations

- Distributer the initial Penetration Testing Report and findings to the Metier Development and Engineering Team.
- Metier response with mitigations and software updates to implement the proposed recommendations and fixes.
- Conduct another assessment and review evidence to validate fixes.
- Perform annual Penetration Testing Assessments for DTAC compliance.

2. Security Findings Summary

The following table lists all the discovered findings with their severity levels. Full technical details of each finding and recommendations can be found in section 3.

2.1. Summary Table of Final Desktop Application Vulnerabilities

Ref #	Finding Description	Severity
3.1.1.	Exposure of Potential Sensitive Data in Logs	Low
3.1.2.	EXE file flagged as malicious	Low
3.1.3.	Lack of Input Validation	Informational

3. Detailed Security Findings, Recommendations and Corrective Actions

3.1. Desktop Application Findings

3.1.1. Exposure of Potential Sensitive Data in Logs

Severity	Low
CVSS	3.4
CVSS String	AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:L/A:N

Description Of Initial Findings:

The application (particularly if configured in debug mode) might store some sensitive information in plain text log files on the local system, including SQL Server credentials (username, password, and server name), patient names, phone numbers etc. Although access is limited, this exposure of sensitive data could present some risk to the organization and its patients.

Affected Resource(s):

- C:\esp\logs

Reference(s):

- https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/
- https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure
- https://owasp.org/www-project-secure-logging-benchmark/
- https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html
- https://cwe.mitre.org/data/definitions/532.html
- https://betterstack.com/community/guides/logging/sensitive-data/
- https://www.skyflow.com/post/how-to-keep-sensitive-data-out-of-your-logs-nine-best-practices
- https://observiq.com/blog/how-to-manage-sensitive-log-data-for-maximum-security

Metier Corrective Actions:

- The ability to configure the software (requires a password) for debug mode has been removed preventing any possibility of Sql usernames/passwords being recorded in logs

- Patient Names have been suppressed from logs

- Telephone Numbers, Clinical System Instance "Windows" Name and user logged in and SQL Instance have been left in logs as these are essential for easy maintenance where remote access is not possible without IT support assistance.

- Mitigation is Telephone numbers are widely used in various other aspects of the telephony system (and the patient has the ability to withhold their number) and the Clinical System in used and User Information (i.e. staff member logged in) are commonly available information on GP Practice Websites.

- Metier are investigating further security/restrictions on accessing the logs folder.

3.1.2. EXE file flagged as malicious

Severity	Low
CVSS	2.0
CVSS String	AV:N/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N

Description:

Upon scanning the executable file "ESPmin2.exe" on VirusTotal, it was flagged as malicious by 2 security vendors (out of 75). These detections identified the file as containing the Trojan W32.AIDetectMalware and Trojan.Malware.300983.susgen.

Both of these threats are types of malware designed to infiltrate systems covertly, potentially leading to unauthorised access, data theft, or system damage.

However, even if these detections are false positives, they still could have a negative impact on customer trust.

Affected Resource(s):

- ESPmin2.exe

Reference(s):

- https://www.virustotal.com/gui/file/ce7c019011dcdf267b4b1e652882807468e9209e29fe5b8337ec3415f54b18b3/detection

Metier Corrective Actions:

- Without further detailed information as to exactly why these 2 Security vendor's analysis flag the software we are unable to investigate further.
- Although a "false positive" we do wish to understand why - the only detail shown in VirusTotal that may explain this is in behavior, it shows the application does read a local text file, this is needed as it allows the ESPmin2.exe main application to know where all of the other applications and configuration files are located if not in the same folder as where ESPMin2.exe is launched from.
- The application is not new and has been deployed to circa 5500 NHS Desk top Computers over the last 14 years - it has never been flagged as malicious by the Antivirus software in use at NHS GP Sites (typically Sophos, Windows Defender, McAfee)

3.1.3. Lack of Input Validation

Severity	Informational

Description:

A lack of input validation arises when an application fails to properly validate user input, thereby permitting attackers to perform unauthorised actions. This vulnerability opens the door for attackers to input potentially harmful data, which could lead to a range of security issues, including injection attacks, data corruption, and unauthorised access to sensitive information. The Custom and Additional Information fields allow users to input data into a field that is subsequently stored and displayed without proper encoding or sanitization. While the injected script is not executed, its persistence within the application's output presents a potential risk. An attacker could exploit this vulnerability to inject malicious scripts that might be executed under specific conditions or in conjunction with other vulnerabilities.

Affected Resource(s):

- Custom Notes Field
- Additional Information Field

Reference(s):

- https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
- https://cwe.mitre.org/data/definitions/20.html
- https://cwe.mitre.org/data/definitions/345.html

Metier Corrective Actions:

- The application does not run in a browser and has no functionality to execute any code entered as text by a malicious user.
- However to eliminate/mitigate this risk, we have updated the software to restrict certain characters being saved in our “notes” field – any of the characters listed below (being those likely to be in any script/program) are replaced with the character “?” on being saved;
    - { and }, [and], < and >, %, .net, .bat, Java

5 Appendices

5.1 Vulnerability Severity Definition

Vulnerabilities are provided with a severity scale that has been individually determined by 8FoldGovernance tester based on the results of the security assessment within the customer's unique environment. Severity is also dependent on the technical impact and the likelihood of discovered findings.

In terms of the likelihood of the vulnerabilities occurring, we recognise that the Call Connect GP software has no reliance on Web browsers and has no web facing functionality so the malicious user would have to gain access to the GP users PC/Windows session.

Severity	Description
Critical	A critical severity vulnerability is defined as one that leads to the full immediate compromise of the system or critically sensitive data.
High	A high severity vulnerability is defined as one that can cause major disruption on a network or target which may lead to the target or sensitive data being compromised.
Medium	A medium severity vulnerability is defined as one that may disclose further information that could lead to an attack or may decrease the overall security of the network or target.
Low	A low severity vulnerability is defined as one that may not be an immediate threat to the company. However, the company should review the information and determine the correct course of action.
Informational	An informational severity vulnerability is defined as one that has no direct security impact but is recommended to be remediated.

5.2 Legal Note and Statement of Limitation

Please note that it is impossible to exhaustively test and identify every possible security vulnerability within the systems in scope. This report does not form a guarantee that the company's assets are 100% secure from all threats. The data shown in the report should not be used alone to judge the security of any computer system. Some scans were performed using automated tools and may not reveal all the possible security weaknesses of the systems in scope. Due to the fast changes in the Information Technology sector, tests performed will exclude vulnerabilities that were identified and published after documenting this report. 8foldGovernance does not guarantee that remediating the vulnerabilities identified makes the assets completely safe from every form of attack.