Office
Automata

Application Code Review Test Report

Prepared By:

Technoally

DOCUMENT CONTROL

Document Properties	
Document Title	Application Code Review Test Report
Category	Confidential
Requestor	OfficeAutomata
File Name	Application Code Review Test Report v1.4
Author	Praveen
Date Created	29-05-2020
Publish Date	02-07-2020

Contents

Objective

The objective of this document is to provide the results of the code review of OfficeAutomata software. Technoally performed the code review of the OfficeAutomata software.

The objective of this code review is to examine the OfficeAutomata software, focusing mainly on its security aspects, the risk that they pose to its users and the integrity and confidentiality of the data contained within.

Summary

This code review was performed by Technoally Team to review aspects of the security and integrity of the OfficeAutomata software. This report identifies the security vulnerabilities that might be exploited to alter OfficeAutomata software, critical data such as client information, or to conduct a sql injection, denial of service attack etc. on the system that were found through decompile exe source code review and by searches of public vulnerability sources.

TERMINOLOGY AND SCORE

The grading of the risk identified is based on the probability and the level of impact of the risk which is assumed based on the discussions and historic data available. It may be noted that a risk grading in the above context reflects the potential that a process or transaction may not achieve its objective or a control breakdown may occur rather than an indication that the risk may have manifested itself in the past. In other words, past history in terms of an event having occurred or not occurred, as the case maybe, in the context of an observation will not indicate that the risk is lower than graded.

CVSS score	Severity in advisory	Description
8.0 – 10	**Critical**	Issues that allow an attacker to run executable code of their choice on the machine, with ease, and without assistance from the user.
		Impact: All services completely lost and no workaround is immediately available. Mission critical data associated with the appliance is disclosed or corrupted.
6.0 – 7.9	**High**	Issues that allow an attacker to run executable code of their choice on the machine, with great difficulty, or requiring significant user interaction.
		Impact: Major functionality of the appliance is severely impaired. Operations can continue in a restricted fashion, although long-term productivity might be adversely affected. Extensive loss or corruption of critical data.
3.0 – 5.9	**Medium**	Issues that require an attacker to reside on the same local network as the victim.
		Impact: Affect only non-standard configurations or obscure applications
0.0 – 2.9	**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.
		Impact: Privacy leaks on non-confidential data, such as dates visited, cached files, visited history, etc.

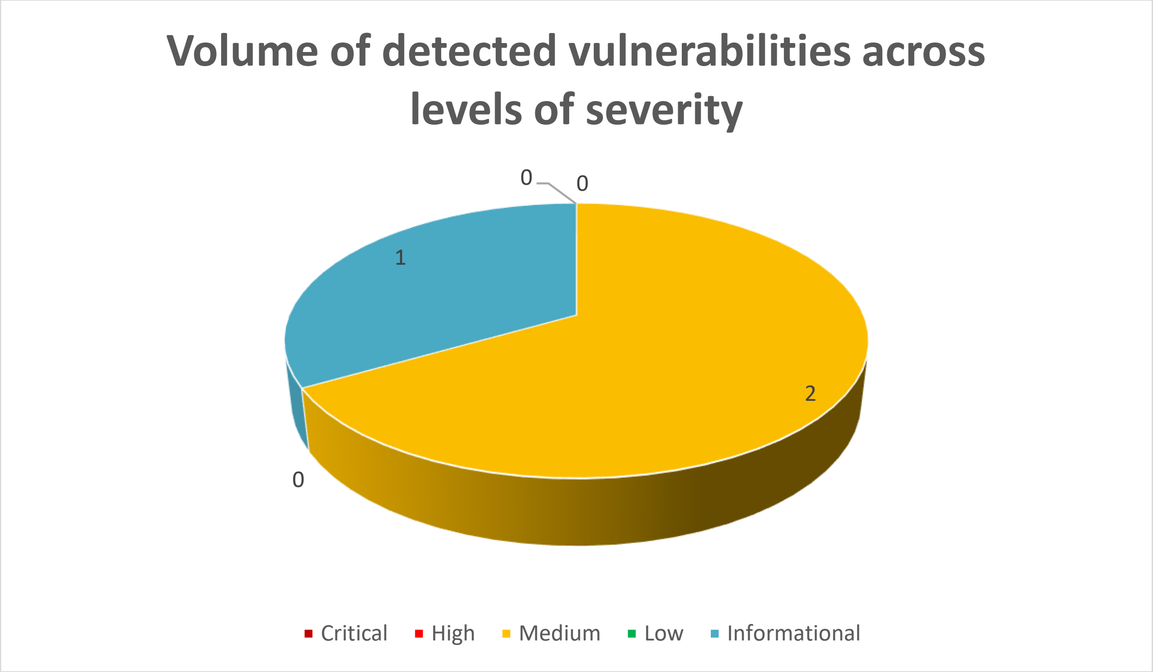
SCOPE OF WORK

The purpose of this assessment is to identify technical as well as logical vulnerabilities on the OfficeAutomata software and provide recommendations for risk mitigation that may arise on successful exploitation of these vulnerabilities.

Sl. No.	Details
1	OfficeAutomata software

Classification by Vulnerability Severity

Volume of detected vulnerabilities across levels of severity



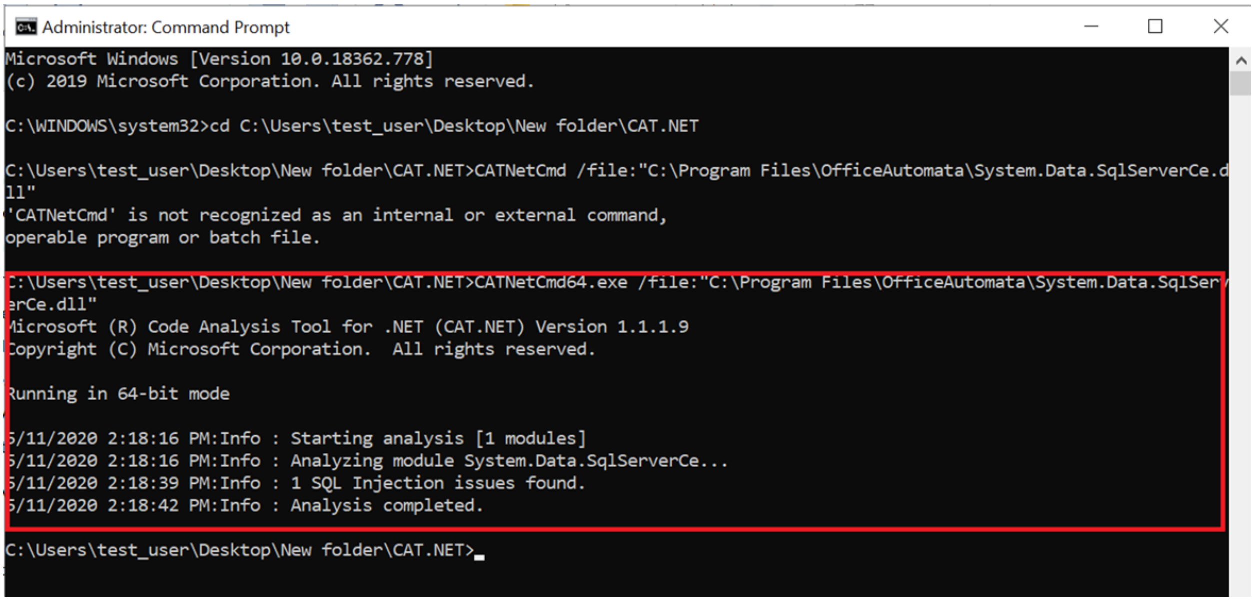
Sl. No.	Severity	Status	Vulnerability
1	Medium	Controlled	SQL Injection
2	Medium	Resolved	Sensitive Data Exposure
3	Informational	Controlled	Possible to modify license duration

VULNERABILITY DETAILS AND MITIGATION

Vulnerability #1: SQL Injection (system.data.sqlserverce.dll)

Vulnerabilities Details	A SQL injection vulnerability was found through a user controlled variable that enters the application. The variable stack which eventually leads to a SQL injection issue.
Severity	Medium
Status	Controlled
Customer Comments	SQL Ce DB is for local user tracking backup only, it has no impact on system security.
Affected Item(s)	C:\Program Files\OfficeAutomata\System.Data.SqlServerCe.dll

Evidence



```
Microsoft Windows [Version 10.0.18362.778]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Users\test_user\Desktop\New folder\CAT.NET

C:\Users\test_user\Desktop\New folder\CAT.NET>CATNetCmd /file:"C:\Program Files\OfficeAutomata\System.Data.SqlServerCe.d
ll"
'CATNetCmd' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\test_user\Desktop\New folder\CAT.NET>CATNetCmd64.exe /file:"C:\Program Files\OfficeAutomata\System.Data.SqlSer
erCe.dll"
Microsoft (R) Code Analysis Tool for .NET (CAT.NET) Version 1.1.1.9
Copyright (C) Microsoft Corporation.  All rights reserved.

Running in 64-bit mode

5/11/2020 2:18:16 PM:Info : Starting analysis [1 modules]
5/11/2020 2:18:16 PM:Info : Analyzing module System.Data.SqlServerCe...
5/11/2020 2:18:39 PM:Info : 1 SQL Injection issues found.
5/11/2020 2:18:42 PM:Info : Analysis completed.

C:\Users\test_user\Desktop\New folder\CAT.NET>
```

Vulnerability #2: Sensitive Data Exposure

Vulnerabilities Details	Application stores information in .sdf file. If these files are not secured, a malicious user can read data from the files. The file could contain sensitive information that could help an attacker to conduct further attacks.
Severity	Medium
Status	Resolved
Affected Item(s)	officeAutomataDatabase.sdf

Informational #3: Possible to modify license duration

Details	An issue was discovered in the source code. The attacker, by modify a field in the AddDays and run the modify source code compile file
Severity	**Informational**
Status	Controlled
Customer Comments	License checks are done on system startup, there are no trial or number of days checks.

CONCLUSION

The application code assessment performed on the OfficeAutomata software, discovered several vulnerabilities which could expose sensitive data. Security assessment revealed that data integrity was at risk which could have led to theft or modification of data and could have had an effect on operations if a malicious party had exploited them. OfficeAutomata has fixed all critical vulnerabilities which could have exposed sensitive data or affected operations.

The analysis also revealed vulnerable areas of medium risk level (100%) that was due to an official Microsoft library for local databases. It has no impact on overall system security as all SQL inserts to this backup offline database are parameterized.

In furtherance of the effectiveness of our vulnerability reporting, we have provided practical guidance for risk mitigation with effective remediation techniques, best practices and tactical approaches to enable optimal security maintenance. These recommendations have been developed with core competency and operational efficiency as prime focus and will be instrumental in achieving sustained threat protection.