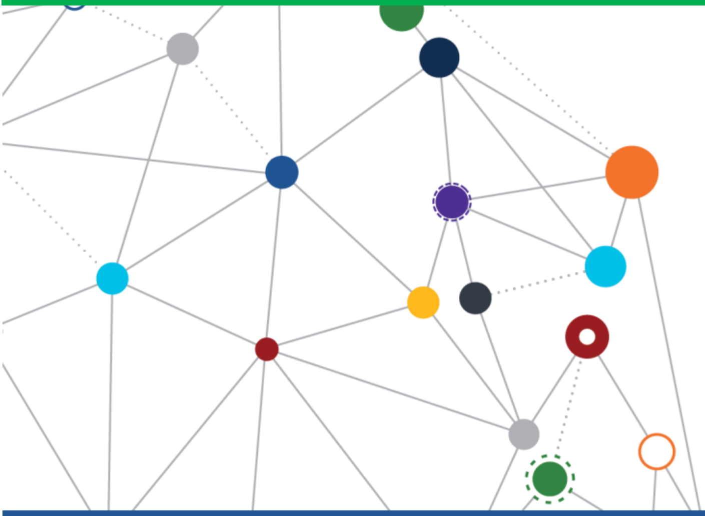
# OIS Fortify Scan Validation Report

Customer Relationship Management - Unified Desktop Optimization (CRM UDO) COTS Solution Custom Modules v2.25.0.0.0.2

Application-ID: 025CFF25-BC3C-432a-B2A5-88602AFDA218
Filename: VA SwA Code Validation CRM UDO v2.25.0.0.0.2 2021-08-02 PASS.pdf

AUGUST 02, 2021 | OIS SOFTWARE ASSURANCE

PASS: This application has successfully completed the Application Security Testing ATO Process.



VA

U.S. Department of Veterans Affairs
Office of Information and Technology
*Office of Information Security*

# Table of Contents

# 1 OIS Fortify Scan Validation Report Introduction

This document contains the results of the validation by OIS Software Assurance of developer-performed scans of Customer Relationship Management - Unified Desktop Optimization (CRM UDO) COTS Solution Custom Modules source code for potential vulnerabilities using the OIS-licensed Fortify tool.

This document contains the following additional sections:

Section 2. **OIS Fortify Scan Validation Results**

This section summarizes the results of the validation.

Section 3. **OIS Fortify Scan Validation Process Details**

This section describes how the validation was performed.

Section 4. **OIS Fortify Scan Validation Findings and Recommendations**

This section contains technical analysis of individual scan findings. Recommendations are also provided.

Section 5. **OIS Fortify Scan Validation Report Conclusion**

This section contains additional recommendations to further increase the ability of the application to protect itself against attacks.

## 1.1 Application Information

The version of Customer Relationship Management - Unified Desktop Optimization (CRM UDO) COTS Solution Custom Modules for which OIS-licensed Fortify scan results were provided was v2.25.0.0.0.2. The following was provided by the developer for review:

1. Completed V&V Secure Code Review Validation Request Form
2. udo_scan_20210728.fpr – Fortify Static Code Analyzer (SCA) static analysis tool scan result file
3. crm-udo-code.zip - Customer Relationship Management - Unified Desktop Optimization (CRM UDO) COTS Solution Custom Modules v2.25.0.0.0.2 source code
4. Additional documentation:
   - FileNotScanned.txt
   - translation_FortifySupport.log
   - scan_FortifySupport.log

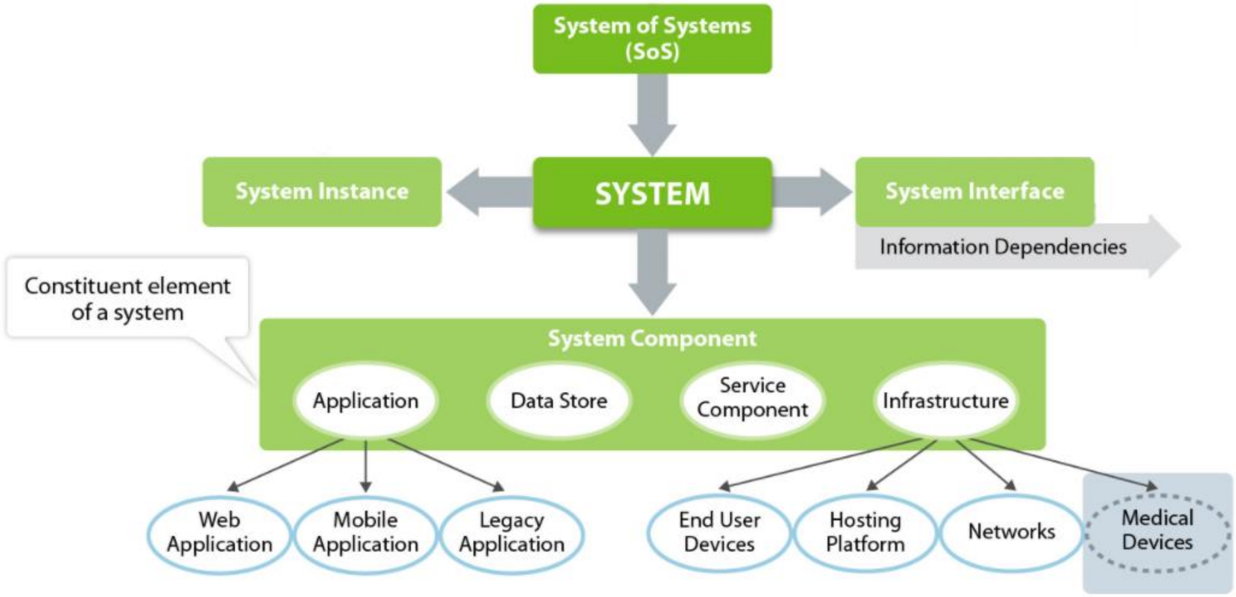
# 2 OIS Fortify Scan Validation Results

This document contains the results of the validation by OIS Software Assurance of developer-performed scans of Customer Relationship Management - Unified Desktop Optimization (CRM UDO) COTS Solution Custom Modules source code for potential vulnerabilities using the OIS-licensed Fortify tool. Fortify SCA static analysis tool scan result files, and of any provided custom scan tool custom rule files, as well as the Customer Relationship Management - Unified Desktop Optimization (CRM UDO) COTS Solution Custom Modules v2.25.0.0.0.2 source code were reviewed.

Using the Fortify tool to scan the source code of custom-developed VA applications, libraries, microservices, and other software components according to OIS Software Assurance guidance is required to meet *Authorization Requirements SOP* “Application Security Testing” ATO requirements. Scans are reviewed by for correctness and completeness, ensuring that that risk-based operations in software are secure.

VA’s business IT systems are a combination of IT hardware, software, and information management capabilities that are aligned with VA strategic goals and business processes as depicted below. OIS Software Assurance’s mission is to increase the security of VA systems by specifically focusing on increasing the ability of VA systems’ to defend themselves against application-level attacks.

**Figure 1. Notional VA system**



VA application developers are required to use the latest version of the OIS-licensed Fortify tool that is redistributed by OIS Software Assurance to scan custom-developed source code for potential vulnerabilities. VA application developers are additionally required to demonstrate their use of Fortify in non-DevSecOps environments as a release gate, and in DevSecOps environments as effectively a CI/CD pipeline certification

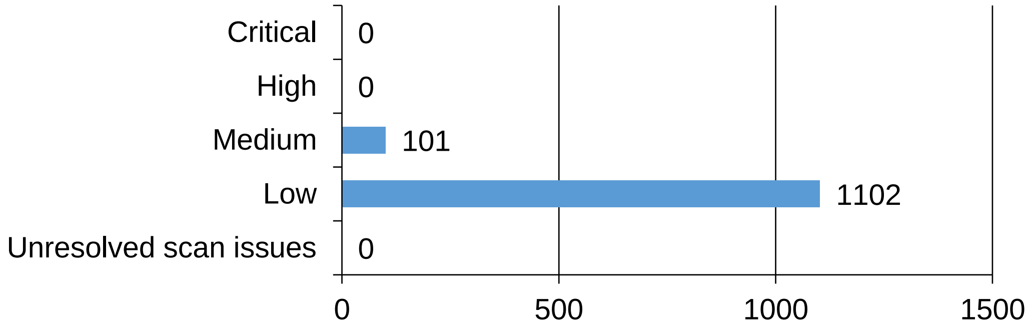
The validation by OIS Software Assurance reviewed provided materials to ensure that:

1. Application information in OIS Fortify scan validation request packages is accurate and complete, and
2. Application scan results demonstrate that OIS Software Assurance guidance has been followed, and
3. Application scan results demonstrate that mitigations must have been made for issues reported by the Fortify tool, and
4. There are justifications provided for cases where Fortify rules are disabled, or scan results are marked as false positives.

For more information about the validation process, see Section 3.

The validation by OIS Software Assurance identified a total of 0 residual vulnerabilities that were considered Critical in severity. There was a total of 0 residual High severity vulnerabilities. There was a total of 101 residual Medium severity vulnerabilities. There was a total of 1,102 residual Low severity vulnerabilities. There was a total of 0 unresolved scan issues.

**Figure 2. Summary of Residual Vulnerabilities & Unresolved Scan Issues**



For more information about residual vulnerabilities and unresolved scan issues that were identified during the OIS Fortify scan validation, see Section 4.

# 3 OIS Fortify Scan Validation Process Details

The OIS Fortify scan validation was performed overall as follows:

**Step 1. Perform initial planning**

The first step that was performed was to perform initial planning. This included developing a strategy for performing the review and identifying considerations that should be considered during the review, such as any Fortify custom rule files provided by the developer.

**Step 2. Review source code**

The next step is to perform the review. A combination of using Fortify to review scan result files and manual analysis was used. The scan results were reviewed to ensure that best practices for performing secure code review have been followed, and that guidance has been followed, as noted in the previous section.

**Step 3. Write report**

The last step in the validation process is to write up the report, after working with the VA application developer to resolve any issues identified during review.

## 3.1 Validation Strategy

The OIS Fortify scan validation was performed by reviewing OIS-licensed Fortify tool scan result files and any provided custom rule files. The provided source code was reviewed as need to support analysis of the provided scan result and custom rule files. The validation included at a minimum the following checks:

**Review developer-provided scan file for matching source code**

This validation check consists of ensuring that the source code matches the uploaded static analysis tool scan result files. While during the comparison there may be some differences such as build files, source code files should not contain any differences.

**Review developer-provided scan file for scanning issues**

This validation check consists of reviewing static analysis tool scan result file for any anomalies in the scan. When running the scan there may have been issues reported by the static analysis tool that affected the quality or completeness of the scan that may have been overlooked.

**Review developer-provided scan file for residual findings**

This validation check consists of ensuring that there are no Critical or High findings in the uploaded static analysis tool scan result file (Fortify ".fpr" extension file) using Fortify Audit Workbench, after first configuring it to use any provided custom rule files.

**Review developer-provided scan file for suppression of issues**

This validation check consists of reviewing static analysis tool scan result files to ensure that issues reported by Fortify have not been suppressed, as opposed to adding comments and developing custom rules as might be appropriate.

**Review developer-provided custom rule files, if provided**

This validation check consists of reviewing any provided static analysis tool custom rule files. Analysis includes examining custom rule files e.g. to ensure that there are no rules to disable built-in Fortify rules, unless those custom rules include documentation justifying their use.

**Perform additional supporting analysis, as needed**

This validation check consists of performing additional supporting analysis for items that may have been identified during the validation for a particular application. For example, findings in the scan result files have been marked as N/A, checks would be performed to ensure there is some documented justification, and to verify the soundness of the justification. Alternately for example, analysis may be performed to determine the appropriateness of exclusions.

## 3.2 Tools Used for Validation

OIS Software Assurance uses the same OIS-licensed Fortify tool as VA application developers. The tool is used in order to promote confidence in the outcome of the validation if the tool is in fact being used during development. Fortify version 21.1.0 was used to review provided static analysis tool scan result and custom rule files. The Audit Workbench tool which is part of Fortify was used to facilitate examining static analysis tool scan result files. Similarly, the Custom Rules Editor tool which is also part of Fortify was used to facilitate examining custom rule files.

## 3.3 Categorization of Findings

The findings that resulted from performing the validation are grouped in Section 4 of this report by severity and type of vulnerability. Findings were rated according to severities reported by the Fortify tool, and/or at the discretion of OIS Software Assurance as follows:

**Findings that are Critical in severity**

Vulnerabilities in source code that must be fixed immediately, for example exposed passwords or Personally-Identifiable Information (PII).

**Findings that are High in severity**

Vulnerabilities in source code that allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.

### Findings that are Medium in severity

Vulnerabilities in source code that provide information that have a high potential of giving access to an intruder.

### Findings that are Low in severity

Vulnerabilities in source code that provide information that potentially could lead to compromise.

### Findings that are unresolved scan issues

This finding categorization is reserved for issues having to do with how the scan was conducted, for example, source code not matching the uploaded static analysis tool scan result files.

### Additional findings

This finding categorization is reserved for any additional concerns identified by the OIS Software Assurance review that do not correspond to the categories above. For example, new issues may be identified during the validation while reviewing supporting documentation.

# 4 OIS Fortify Scan Validation Findings and Recommendations

## 4.1 Residual Critical Findings (0 Total)

Based on the information provided by the developer, it does not appear that vulnerabilities identified by Fortify that were Critical in severity were left unmitigated.

| CWE-ID | CWE-Title | Number of Instances | Notes |
|---|---|---|---|
| CWE-601 | Open Redirect | 0 | **udo_controlpanel.js**<br>**Closed**<br>Agree despite developer analysis.<br>This finding is closed because there is validation to ensure the user is redirected to a va.gov site. There is additional validation to ensure the path includes "/dac/vva".<br>**udo_PeopleLauncher.js:**<br>**Closed**<br>Agree despite developer analysis.<br>Part of the URL is hardcoded in the switch statement. This will ensure a user cannot be redirected to any site. However, it is strongly encouraged to URL encode the value appended to the query string.<br>**WebApiClient.min.js(2)**<br>**Closed**<br>Agree despite developer analysis.<br>It is demonstrated that the code is using a recommended approach for communicating with a Dynamics CRM OData endpoint. Also, other findings |

| | | | |
|---|---|---|---|
| | | | state the code is communicating over an encrypted channel (HTTPS) with a known CRM endpoint. Lastly, it has been stated that the code is retrieving a field stored within a CRM system, not entered directly by the end user within the UI.<br>Note that it is recommended to merge new scans with previously audited FPR files. This will retain the audit comment history and help ensure issues remain closed.  Please see this technical note for more information. |
| CWE-359 | Privacy Violation | 0 | **Closed**<br>Accept developer analysis.<br>The data appears to be protected appropriately while in transit and at rest.  The data is sent over HTTPS and the developer provided this documentation to show that the data is stored encrypted while at rest:<br>https://docs.microsoft.com/en-us/microsoft-365/compliance/office-365-encryption-in-microsoft-dynamics-365?view=o365-worldwide#:~:text=All%20instances%20of%20Dynamics%20365,SQL%20Data%20Warehouse%20 |
| CWE-91 | XML Injection | 0 | **Closed**<br>Agree despite developer analysis.<br>It is demonstrated that the code is using a recommended approach for communicating with a Dynamics CRM OData endpoint. Also, other findings state the code is communicating over an encrypted channel (HTTPS) with a known CRM endpoint. Lastly, it has been stated that the code is retrieving |

| | | | |
|---|---|---|---|
| | | | a field stored within a CRM system, not entered directly by the end user within the UI. |

## 4.2 Residual High Findings (0 Total)

Based on the information provided by the developer, it does not appear that vulnerabilities identified by Fortify that were High in severity were left unmitigated.

| CWE-ID | CWE-Title | Number of Instances | Notes |
|---|---|---|---|
| CWE-79, CWE-80 | Cross-Site Scripting: DOM | 0 | **Closed**<br>Agree despite developer analysis.<br>It is demonstrated that the code is using a recommended approach for communicating with a Dynamics CRM OData endpoint. Also, other findings state the code is communicating over an encrypted channel (HTTPS) with a known CRM endpoint. Lastly, it has been stated that the code is retrieving a field stored within a CRM system, not entered directly by the end user within the UI. |
| CWE-338 | Insecure Randomness | 0 | **Closed**<br>Accept developer analysis.<br>The math.random function is not being used in a security context. |
| CWE-918 | Server-Side Request Forgery | 0 | **Closed**<br>Accept developer analysis.<br>The documentation for the IOrganizationService.Create(Entity) Method (https://docs.microsoft.com/en-us/dotnet/api/microsoft.xrm.sdk.iorganizationservice.create?view=dynamics- |

| | | | |
|---|---|---|---|
| | | | general-ce-9#Microsoft_Xrm_Sdk_IOrganizationService_Create_Microsoft_Xrm_Sdk_Entity_)<br>states ,“To perform this action, the caller must have privileges on the entity that is specified in the entity parameter.” This indicates that Dynamics CRM performs validation that the caller has the correct privileges for the action, which should mitigate the possibility of server-side request forgery.<br>Note that it is recommended to merge new scans with previously audited FPR files. This will retain the audit comment history and help ensure issues remain closed. Please see this technical note for more information. |

## 4.3 Residual Medium Findings (101 Total)

The vulnerabilities below were identified by Fortify that were Medium in severity were left unmitigated and are still being reported by Fortify. It is estimated that it will take approximately 26 hours to address the following issues.

| CWE-ID | CWE-Title | Number of Instances | Notes |
|---|---|---|---|
| CWE-11 | ASP.NET Misconfiguration: Debug Information | 23 | This issue has not been audited. |
| CWE-12 | ASP.NET Misconfiguration: Missing Error Handling | 47 | This issue has not been audited. |

| | | | |
|---|---|---|---|
| CWE-554 | HTML5: MIME Sniffing | 31 | This issue has not been audited. |

## 4.4 Residual Low Findings (1,102 Total)

The vulnerabilities below were identified by Fortify that were Low in severity were left unmitigated and are still being reported by Fortify. It is estimated that it will take approximately 276 hours to address the following issues.

| CWE-ID | CWE-Title | Number of Instances | Notes |
|---|---|---|---|
| CWE-486 | Code Correctness: Erroneous Class Compare | 19 | This issue has not been audited. |
| CWE-398 | Code Correctness: Misleading Method Signature | 1 | This issue has not been audited. |
| CWE-730 | Code Correctness: Missing [Serializable] Attribute | 2 | This issue has not been audited. |
| CWE-398 | Code Correctness: ToString on Array | 2 | This issue has not been audited. |
| CWE-1004 | Cookie Security: HTTPOnly not Set on Application Cookie | 279 | This issue has not been audited. |
| CWE-352 | Cross-Site Request Forgery | 13 | This issue has not been audited. |
| CWE-82,<br>CWE-83,<br>CWE-87,<br>CWE-692 | Cross-Site Scripting: Poor Validation | 1 | This issue has not been audited. |

| | | | |
|---|---|---|---|
| CWE-561 | Dead Code: Unused Field | 66 | This issue has not been audited. |
| CWE-561 | Dead Code: Unused Method | 105 | This issue has not been audited. |
| CWE-730 | Denial of Service | 5 | This issue has not been audited. |
| N/A | JavaScript Hijacking | 3 | This issue has not been audited. |
| CWE-581 | Object Model Violation: Just One of Equals() and GetHashCode() Defined | 1 | This issue has not been audited. |
| CWE-259 | Password Management: Null Password | 7 | This issue has not been audited. |
| CWE-615 | Password Management: Password in Comment | 25 | This issue has not been audited. |
| CWE-1069 | Poor Error Handling: Empty Catch Block | 111 | This issue has not been audited. |
| CWE-396 | Poor Error Handling: Overly Broad Catch | 391 | This issue has not been audited. |
| CWE-398 | Poor Logging Practice: Use of a System Output Stream | 1 | This issue has not been audited. |
| CWE-215,<br>CWE-489,<br>CWE-497 | System Information Leak: External | 2 | This issue has not been audited. |

| | | | |
|---|---|---|---|
| CWE-497 | System Information Leak: Internal | 64 | This issue has not been audited. |
| CWE-252, CWE-754 | Unchecked Return Value | 4 | This issue has not been audited. |

## 4.5 Issues with How Scans Were Performed (0 Total)

### *4.5.1 Unresolved Scan Issues*

Based on the information provided, it does not appear that there were unresolved issues when the scan of the source code was conducted.

### *4.5.2 Informational Scan Issues*

| Description of Concern |
|---|
| These are informational issues having to do with how the scan was conducted by the developer. They are not counted against passing and are listed here for reference only. These issues may have impacted the ability of Fortify to identify Critical, High, Medium, or Low in severity findings. Descriptions of the scan issues, and recommendations for each, are below. |
| **Details** |

| | ***Issue*** | ***Description*** | ***Recommendation*** |
|---|---|---|---|
| 1. | New version of Fortify available | A new version of Fortify (21.1.0) was released recently. Future code review submissions should utilize the new version of Fortify. | This issue is not included in the count of scan issues. Download the latest Fortify version from Teams. |
| 2. | Source code not scanned | All source code must be scanned by Fortify and that does not appear to be the case in this validation submission package. | This issue is not included in the count of scan issues. Since the developer has explained why these files were not scanned in the |

| | | |
|---|---|---|
| | See Appendix A for a full listing of the files that were delivered for review but were not scanned by Fortify. | provided documentation - FileNotScanned.txt. This issue is not counted against passing. Please ensure this documentation is included in future submissions. See this technical note for reference. |
| | | |

## 4.6 Additional Findings (0 Total)

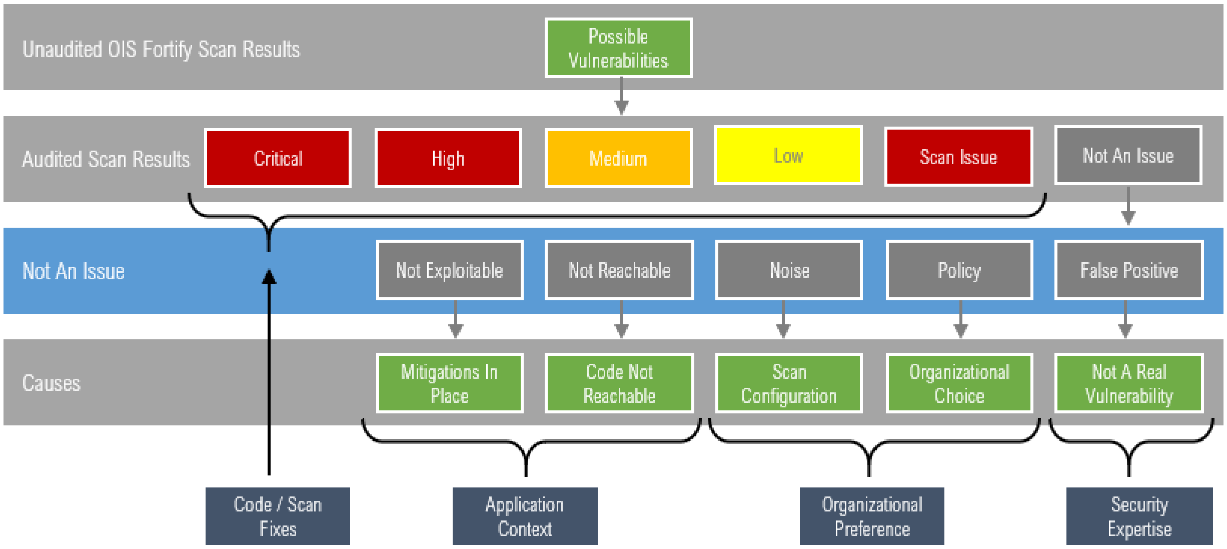
There were no additional findings that were identified during the course of the validation.

# 5 OIS Fortify Scan Validation Report Conclusion

Building secure custom-developed VA applications, libraries, microservices, and other software components is every VA application developer's responsibility. Application-level vulnerabilities generally manifest themselves as one of two types: design flaws introduced by weaknesses during the requirements, design, or architecture phase; or implementation bugs introduced by weaknesses during the actual coding of the application.

The OIS-licensed Fortify tool should be used according to OIS Software Assurance guidance to scan source code for potential vulnerabilities that manifest themselves as implementation bugs as depicted in the figure below. Fortify supports a wide range of programming languages and build environments. Fortify can also be used as a standalone tool by VA developers, or integrated into for example Continuous Integration (CI) build environments.

**Figure 3. Notional OIS Fortify scan results and types of analysis required**



OIS Software Assurance uses the same OIS-licensed Fortify tool as VA application developers to promote confidence in the outcome of the validation if the tool is in fact being used during development. Remediation estimates are provided to assist with planning remediation work, if or as might be appropriate. Some bugs will be harder to fix than others. For example, modifying a single line of code in a self-contained method is easier than modifying the result of a sequence of calls.

## 5.1 Resources that you may find helpful

The following resources may be helpful to readers of this report:

**Microsoft Teams OIS Software Assurance support team**

This OIS Software Assurance resource provides technical guidance for using the OIS-licensed Fortify tool and for reviewing scan results.

**OIS-licensed Fortify tool product documentation**

This vendor resource provides product documentation for the OIS-licensed Fortify tool, including installation and configuration guidance, and user guidance.

**OIS eMASS Knowledge Service**

This OIS resource provides information about VA’s GRC tool eMASS, including the latest version of the Authorization Requirements SOP document.

# Appendix A Source Code Not Scanned

The following files were delivered for review but were not scanned by Fortify:

UDO.D365\UDO.D365.Plugins\PluginBase.cs

UDO.D365\UDO.D365.Plugins\UDO.D365.Plugins\PluginBase.cs

UDO.LOB\UDO.Crm.LOB.Core\Interfaces\ITimedProcessor.cs

UDO.LOB\UDO.Crm.LOB.Extensions\Interfaces\ILegacyHeaderInfo.cs

UDO.LOB\UDO.Crm.LOB.Extensions\Interfaces\IUDOException.cs

UDO.LOB\UDO.Crm.LOB.Extensions\Interfaces\IUDORequest.cs

UDO.LOB\UDO.LOB.Core\Constants\CommonResponseMessages.cs

UDO.LOB\UDO.LOB.Core\Interfaces\ILegacyHeaderInfo.cs

UDO.LOB\UDO.LOB.Core\Interfaces\ITimedProcessor.cs

UDO.LOB\UDO.LOB.Core\Interfaces\IUDOException.cs

UDO.LOB\UDO.LOB.Core\Interfaces\IUDORequest.cs

UDO.LOB\UDO.LOB.Core\Models\ApiCatalog.cs

UDO.LOB\UDO.LOB.Core\Models\MessageBase.cs

UDO.LOB\UDO.LOB.Core\Models\UDOHeaderInfo.cs

UDO.LOB\UDO.LOB.Core\Models\UDORelatedEntity.cs

UDO.LOB\UDO.LOB.Core\Models\UDORequestBase.cs

UDO.LOB\UDO.LOB.Core\Models\UDOResponseBase.cs

UDO.LOB\UDO.LOB.DependentMaintenance\Plugins\Util\Util.cs

UDO.LOB\UDO.LOB.DependentMaintenance\VRM.Integration.Servicebus.Bgs.Messages\Properties\VersionInfo.cs

UDO.LOB\UDO.LOB.DependentMaintenance\VRM.Integration.Servicebus.Bgs.Services\Properties\VersionInfo.cs

UDO.LOB\UDO.LOB.DependentMaintenance\VersionInfo.cs

UDO.LOB\UDO.LOB.Extensions\ApiCatalogManager.cs

UDO.LOB\UDO.LOB.Extensions\CRM\ConnectionSettings.cs

UDO.LOB\UDO.LOB.Extensions\CRM\CrmConfiguration.cs

UDO.LOB\UDO.LOB.Extensions\CRM\CrmConnection.cs

UDO.LOB\UDO.LOB.Extensions\CRM\EntityCache.cs

UDO.LOB\UDO.LOB.Extensions\CRM\ExecuteMultipleHelper.cs

UDO.LOB\UDO.LOB.Extensions\CRM\ExecuteMultipleHelperSettings.cs

UDO.LOB\UDO.LOB.Extensions\CRM\MethodInfo.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Client\AutoRefreshSecurityToken.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Client\Enums.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Client\ILocalResults.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Client\ManagedTokenServiceProxy.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Client\ParallelOperationContext.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Client\ParallelOperationFailure.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Client\ParallelServiceProxy.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Client\ServiceProxyOptions.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Client\XrmServiceManager.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Client\XrmServiceUriFactory.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\ConnectionManager.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\CrmServiceClientAuthOverride.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Diagnostics\ExtensionMethods.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Diagnostics\XrmCoreEventSource.Authentication.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Diagnostics\XrmCoreEventSource.Parallel.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Diagnostics\XrmCoreEventSource.Query.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Diagnostics\XrmCoreEventSource.Service.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Diagnostics\XrmCoreEventSource.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Diagnostics\XrmCoreEventSourceEventIds.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Extensions\BatchRequestExtensions.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Extensions\QueryExtensions.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Extensions\SecurityExtensions.cs

UDO.LOB\UDO.LOB.Extensions\CRM\PfeCore\Extensions\ServiceExtensions.cs

UDO.LOB\UDO.LOB.Extensions\CRM\SecurityTools.cs

UDO.LOB\UDO.LOB.Extensions\CRM\TimeTracker.cs

UDO.LOB\UDO.LOB.Extensions\CRM\TimedProcessor.cs

UDO.LOB\UDO.LOB.Extensions\CRM\Tools.cs

UDO.LOB\UDO.LOB.Extensions\CRM\TruncHelperSettings.cs

UDO.LOB\UDO.LOB.Extensions\CRM\TruncateFields.cs

UDO.LOB\UDO.LOB.Extensions\Interfaces\ILegacyHeaderInfo.cs

UDO.LOB\UDO.LOB.Extensions\Interfaces\ITimedProcessor.cs

UDO.LOB\UDO.LOB.Extensions\Interfaces\IUDOException.cs

UDO.LOB\UDO.LOB.Extensions\Interfaces\IUDORequest.cs

UDO.LOB\UDO.LOB.Extensions\JsonHelper.cs

UDO.LOB\UDO.LOB.Extensions\Logging\AiLogger.cs

UDO.LOB\UDO.LOB.Extensions\Logging\AppInsightsExtentions.cs

UDO.LOB\UDO.LOB.Extensions\Logging\IAiLogger.cs

UDO.LOB\UDO.LOB.Extensions\Logging\LogHelper.cs

UDO.LOB\UDO.LOB.Extensions\Logging\TraceLogger.cs

UDO.LOB\UDO.LOB.Extensions\Security\AzureAccessToken.cs

UDO.LOB\UDO.LOB.Extensions\Security\AzureAuthResult.cs

UDO.LOB\UDO.LOB.Extensions\Security\AzureAuthenticationHelper.cs

UDO.LOB\UDO.LOB.Extensions\Security\CRMAuthTokenConfiguration.cs

UDO.LOB\UDO.LOB.Extensions\Security\IAzureAuthenticationHelper.cs

UDO.LOB\UDO.LOB.Extensions\Utility.cs

UDO.LOB\UDO.LOB.Extensions\VEIS\VEISConfiguration.cs

UDO.Plugins\CustomActions.Plugins\Messages\HeaderInfo.cs

UDO.Plugins\CustomActions.Plugins\Messages\PersonSearch\CorrespondingIDs.cs

UDO.Plugins\CustomActions.Plugins\Messages\PersonSearch\IPersonSearchRequest.cs

UDO.Plugins\CustomActions.Plugins\Messages\PersonSearch\IPersonSearchResponse.cs

UDO.Plugins\CustomActions.Plugins\Messages\PersonSearch\IUDOException.cs

UDO.Plugins\CustomActions.Plugins\Messages\PersonSearch\IUDORequest.cs

UDO.Plugins\CustomActions.Plugins\Messages\PersonSearch\Name.cs

UDO.Plugins\CustomActions.Plugins\Messages\PersonSearch\PatientAddress.cs

UDO.Plugins\CustomActions.Plugins\Messages\PersonSearch\PatientPerson.cs

UDO.Plugins\CustomActions.Plugins\Messages\PersonSearch\UDOpsFindPersonRequest.cs

UDO.Plugins\CustomActions.Plugins\Messages\PersonSearch\UDOpsFindPersonResponse.cs

UDO.Plugins\CustomActions.Plugins\Messages\PersonSearch\UnattendedSearchRequest.cs

UDO.Plugins\CustomActions.Plugins\Messages\UDOException.cs

UDO.Plugins\CustomActions.ServiceRequests.Plugins\Messages\HeaderInfo.cs

UDO.Plugins\CustomActions.ServiceRequests.Plugins\Messages\PersonSearch\IUDOException.cs

UDO.Plugins\CustomActions.ServiceRequests.Plugins\Messages\PersonSearch\IUDORequest.cs

UDO.Plugins\CustomActions.ServiceRequests.Plugins\Messages\PersonSearch\UnattendedSearchRequest.cs

UDO.Plugins\CustomActions.ServiceRequests.Plugins\Messages\UDOException.cs

UDO.Plugins\CustomActions.ServiceRequests.Plugins\Messages\VEIS\Core\EcMessageBase.cs

UDO.Plugins\CustomActions.ServiceRequests.Plugins\Messages\VEIS\Core\IMessageBase.cs

UDO.Plugins\CustomActions.ServiceRequests.Plugins\Messages\VEIS\Core\MessageBase.cs

UDO.Plugins\CustomActions.ServiceRequests.Plugins\Messages\VEIS\Core\VEISMessageBase.cs

UDO.Plugins\Va.Udo.Crm.CADD\CADDPlugins\Messages\HeaderInfo.cs

UDO.Plugins\Va.Udo.Crm.VBMSeDocumentService\HeaderInfo.cs