OSCAR- EMR Analysis- Seven Bugs

FINAL REPORT

Contributing to your success

Week 6 –2014/12/22

Contents

1 Background

OntarioMD retained RiskView, with the agreement and cooperation of OSCAR EMR, to conduct an independent review of seven critical or high priority bugs (hereafter referred to as “seven bugs”) in the OSCAR 12.1.1 software of concern to physicians. OSCAR 12.1.1 (Affiliated Product) is the version that is eligible for funding under the Ontario EMR Adoption Program at the time of the review.

The RiskView review uses a structured framework based on best practices in Software Development and IT security, to provide an independent review of the seven bugs in OSCAR 12.1.1. The seven bugs in scope were selected by OntarioMD and sourced from SourceForge. These bugs are: 3392, 3237, 3174, 3110, 2575, 2867, and 3428. In addition, Riskview conducted three key informant interviews with Approved OSCAR Service Providers (Approved OSP) and the OSCAR EMR team to gain a better understanding of the OSCAR 12.1.1 (Affiliated Product) context.

RiskView produced two documents for the scope of this engagement:

1. A technical summary of the review of the seven bugs in the OSCAR-EMR 12.1.1 application which includes an outline of the project scope, approach, summary report for the seven bugs, an overall observation and future recommendation.
2. A summary report of the seven bugs. A detailed bug report for each of the seven bugs runtime behavior and code was provided as supporting documentation. An automated code review report was added as additional value and provided to OSCAR EMR to inform its ongoing code management. (This document)

An automated code review report was added as additional value and provided to OSCAR EMR to inform its ongoing code management.

1.1 Scope

RiskView was asked to perform a deep dive comparative (before and after) analysis for the seven bugs (3237, 3428, 3392, 3174, 3110, 2575, 2867). The objective of this deep dive was to validate the bug fix in order to confirm OSCAR EMR’s assertion that the seven bugs were fixed, as per and within the parameters of RiskView’s engagement.

In parallel:

- A general broad-based scan of the code was conducted using automated software tools as well as a general examination of the relationship between the OSCAR EMR application and its dependant infrastructure.
- Relevant coding “hot spots” identified by the automated software tool were manually verified by the RiskView team and shared with the OSCAR EMR development team for further verification. RiskView does not purport to have completed a comprehensive assessment of the coding hot spots.
- Key informant interviews were also used to inform areas of examination.

1.2 Approach

The RiskView approach is based on years of experience in reviewing mission-critical applications for security and code quality. Measures such as security and code quality are often used as proxies - in eHealth applications for

risks to patient safety; in Finance applications for risks to the commercial transition; and in Industrial / Manufacturing for risks to operator safety.

RiskView uses a multi-pass, multi-prong, automated and manual approach to identify security and code quality related issues:

- **Multi-prong**: We use both Black-Box and White-Box techniques during our review. The Black-Box technique is primarily used to assess the runtime behaviour of an application while in use. The White-Box technique refers to the architecture, design, and the source code review of an application. To increase our confidence level, we set up two runtime environments for each bug in scope. We set up a "Before" and an "After" runtime environment to validate both the existence and the elimination of a bug.
- **Automated and Manual**: We use both automated and manual application review techniques and tools. We use "Automated" application review tools and techniques to provide broad coverage of the code and identify hotspots. We use Manual application review techniques to identify hotspots and refine our findings, build hypotheses and verify them manually.
- **Multi-pass:** We use a multi-pass approach where we examine an application and our hypothesis incrementally. Each increment will build upon the previous passes and helps us further refine our findings and their root causes.

1.3 Disclaimer / Parameters of Investigation

The RiskView review is based on:

- A time boxed study of the seven bugs
- Contributing input from the OSCAR Development team and key information interviews
- Test data supplied to RiskView by OSCAR EMR

Therefore, the analysis does not include all the possible boundary conditions and scenarios for the seven bugs. The RiskView validation of the bugs in scope is on a best efforts basis, using the steps documented by OSCAR EMR in their SourceForge bug reporting system.

2 Executive Summary

OntarioMD's management requested that RiskView validate the OSCAR EMR's assertion that OSCAR Version 12.1.1 (Affiliated Product) contains no residual risk to patient safety because the OSCAR EMR team resolved the seven bugs (*3392, 3237, 3174, 3110, 2575, 2867, and 3428)*

According to OSCAR EMR, Version 12.1.1 (Affiliated Product):

- Was first released on February 20th, 2014.
- Was not widely installed until May 2014.
- Has 869 known installations (i.e. installations *reported to* OSCAR EMR by the Oscar Service Providers.)
- May have broader unreported install base.

It should be noted that in the current model, OSCAR EMR relies on reporting by the Approved OSCAR Service Providers/OSCAR Self-Service Providers to know which version is installed at which physician client as OSCAR

EMR itself does not provide support directly to end user physicians. The version is verified by a Traceability Report received from the Approved OSP and confirmed by OSCAR EMR prior to confirming an installation or upgrade as complete.

Applying a multi-prong, multi-pass approach using both automated and manual assessment techniques to validate the resolution of these bugs, the RiskView validation confirms that within the parameters of RiskView engagement all seven bugs are fixed.

This conclusion was reached by RiskView performing:

- Pre and post (fix) validation for each bug to ensure that the bug was understood and verified.
    - As part of our Runtime (Black-box) analysis, we reproduced each bug in our scope. We also validated their resolution. All bugs successfully passed the documented steps in SourceForge.
    - As part of our Static (White-box) analysis, we performed automated and manual code review.
- Key informants interviews to gain a better appreciation of the context of the application.
    - To gain contextual understanding, RiskView conducted interviews with two OSPs (Indivica and KAIInnovations) and the OSCAR development team. While there is room for improvement, we understand that OSCAR-EMR has made progress in establishing the appropriate processes and tools to better manage the overall quality of their software.
- A high level analysis of the existing bugs in the SourceForge bug tracking repository. We noticed good processes and tools for bug prioritization and resolution.

However, improvement opportunities exist:

- There are improvement opportunities for software inventory management, patching and incident management processes.
- For the Affiliated Product, OSCAR EMR has no direct access to their end users' software installations. Therefore, OSCAR-EMR must rely on Approved OSPs for the installation and patching of their software. Lack of direct access to end users' installations complicates emergency maintenance of OSCAR-EMR.
- RiskView notes that OSCAR-EMR assumes a secure operating environment (infrastructure) where there are adequate policies, procedures, awareness, and technology controls in place. OSCAR-EMR should consider a secure-in-depth strategy with multiple layers of security controls built into the software to prevent accidental or malicious security breaches. Specifically, as OSCAR relies on a secure operating infrastructure failure to successfully implement the appropriate policies, procedures, and technology controls in a secure-in-depth strategy may result in accidental or malicious security breaches.

3 Findings

RiskView confirms that all seven bugs in our scope (SourceForge: 3392, 3237, 3174, 3110, 2575, 2867, and 3428) are fixed within the scope and parameters of our engagement. Below, we have summarized the results of our runtime and code review analysis. Additional and supporting documentation provide further analysis of the runtime behaviour and the corresponding code.

The following table is a summary of our findings. For further technical details we invite you to review our supporting documentation.

Bug #	Bug Description	Status	Bug Scope
2575	Measurement Links in Labs Displaying Values for the Wrong Measurement Type. The historic list of measurement values that pops up when a measurement name is clicked within a lab result is displaying the wrong values - it's showing the values for a different measurement type, not the measurement type indicated in the name/link. An example would be eGFR; when you click eGFR, it displays values for creatinine, not eGFR. See attachment.	**OSCAR EMR Status:** • Closed-Fixed **Third Party Validation:** • Before Build: 407 – Failed • After Build: 445 - Passed • Version 12.1.1.51 • Source: labDisplay.jsp	**Number of physicians patched** 869 **Number of unpatched physicians** 0 **Number of physicians / patient records affected by the bug** Unknown[1]
2867	Lab up-loader rejecting (Occasionally) files after #213 LAB_NOMATCH_NAMES reversion. To reproduce: 1. Open a CML file with a HIN that matches a demographic in the database but alter the year or month or day of birth or the gender so it does not match 2. LAB_NOMATCH_NAMES=yes (this may not matter actually but is my property file setting) 3. upload the file An error occurs and is silently consumed thereby deleting all the HL7 messages in that file, rather than filing all the correct ones, and accepting the one correct HIN and leaving it unmatched (as you would expect)	**OSCAR EMR Status:** • Closed- Fixed **Third Party Validation:** • Before Build: 261– Failed • After Build: 445 – Passed • Version 12.1.1.51 • Source: MessageUploader.java	**Number of physicians patched** 869 **Number of unpatched physicians** 0 **Number of physicians / patient records affected by the bug** Unknown[1]

3110	Information contained within the "NTE" segment of LifeLabs lab results isn't being displayed in OSCAR. The NTE segment contains "Notes and Comments" and is present in certain lab results. A screenshot of a LifeLabs lab with the information in the NTE segment highlighted is attached along with a sample HL7 file.	**OSCAR EMR Status:** • Closed-Fixed **Third Party Validation:** • Before Build: 390 – Failed • After Build: 445 – Passed • Version 12.1.1.51 • Source: MDSHandler.java	**Number of physicians patched** 869 **Number of unpatched physicians** 0 **Number of physicians / patient records affected by the bug** Unknown[1]
3174	When a Lifelabs report is uploaded through mule, the Lifelab client application expects a CURHST.0 log to be created by the EMR upload tool (in this case Mule). However mule is unable to generate this file anymore which means all 12.1.1 users are risking the loss of Lifelabs integration and all new installations of 12.1.1 would be denied Lifelabs electronic reports as non-compliant.	**OSCAR EMR Status:** • Closed-Fixed **Third Party Validation:** • Before Build: 369 – Failed • After Build: 445 – Passed • Version 12.1.1.51 • Source: LabUploadAction.java	**Number of physicians patched** 869 **Number of unpatched physicians** 0 **Number of physicians / patient records affected by the bug** Unknown[1]
3237	CML labs are matched to the wrong patient.	**OSCAR EMR Status:** • Closed-Fixed **Third Party Validation:** • Before Build: 379 – Failed • After Build: 445 – Passed • Version 12.1.1.51 • Source: CMLHandler.java	**Number of physicians patched** 869 **Number of unpatched physicians** 0 **Number of physicians / patient records affected by the bug** Unknown[1]
3392 & 3428	Intermittently, labs will display the wrong lab result information in the results section. Patient name, birthday, and all other information in the header is correct, only the results section displays incorrect values.	**OSCAR EMR Status:** • Closed-Fixed **Third Party Validation:** • Before Build: 407 – Failed • After Build: 445 – Passed • Version 12.1.1.51 • Source: CMLHandler.java	**Number of physicians patched** 869 **Number of unpatched physicians** 0 **Number of physicians / patient records affected by the bug** 15 – confirmed no impact on patient care.

Notes:

1. According to the OSCAR EMR team:

    - OSCAR EMR relies on reporting from Approved Oscar Service Providers to track the number of physicians that use OSCAR 12.1.1. This software is an Affiliated Product of OSCAR EMR once the OSCAR EMR Terms of Use are signed which places the software within the scope of OSCAR EMR's Quality Management System and oversight. As of December 13, 2014, 519 physicians have completed the OSCAR EMR Terms of Use to register their software with OSCAR EMR as an Affiliated Product.
    - To determine the scope of physicians / patient records potentially affected by the bug, each Approved OSCAR Service Provider and Approved OSCAR Self Service Provider would need to provide log information to the OSCAR EMR team. This was not completed within the time frame of this report, however, OSCAR EMR has refined and further strengthened its processes in this regard as follows (excerpt from report from OSCAR EMR to OntarioMD November 21, 2014):

        i. **Communication** – Upon reviewing management of Bug 3392, OSCAR EMR identified the need for more specific communication with Approved OSP/OSSPs related to bugs classified as high or critical. While all information is publically available at all times, and those involved with installing and supporting OSCAR regularly check SourceForge for updates, OSCAR EMR has implemented a specific communication protocol to directly notify all Approved OSP/OSSPs and the open-source developer list of all high and critical bugs as soon as identified and classified. The protocol further requires all Approved OSP/OSSPs to confirm receipt of notification, to assess impact to customers, and to ensure affected customers are notified of any related risk and available temporary workaround.

        ii. **Reporting** – OSCAR EMR has also implemented a more formal reporting process for Approved OSP/OSSPs to specifically confirm deployment of a fix for a high or critical bug to affected customers.