NSW Electoral Commission | iVote

iVote project

Code review report 2021

Published as at
November 2021

Contents

Introduction

The iVote system is to be offered at the December 2021 NSW Local Government elections (LGE), which were postponed from 2020. An updated version (1.8.5) of iVote has been implemented to support local government elections for the first time.

Demtech Group, who conducted a review of the iVote source code in 2019, were asked to review the updated source code, including the following analysis:

- **Code Scanning.** Apply automatic code scanning tools (FindBugs) to identify any vulnerabilities and other problems with the iVote code.
- **Detailed Code Review.** In depth matching between implementation and specification, to the extent possible given design documentation.
- **Verifiability analysis.** Analyse the implementation regarding the relevant artefacts, in particular zero-knowledge proofs.
- **Security analysis.** A security audit of the code to the extent possible.

The scope of the review was the iVote Voting and Assurance System application software delivered by Scytl.

Demtech provided a written report on the findings of the review which is provided as an embedded PDF in Attachment A. Scytl also provided a response to the findings, which is similarly included in Attachment B.

This document covers the NSW Electoral Commission response to the review and is aimed at a non-technical audience.

An overview of the iVote® System[1] is provided on the NSW Electoral Commission website.

[1] Registered trademark of the State of NSW (New South Wales Electoral Commission).

Executive overview

Demtech concluded that the code had not undergone major changes since 2019, aside from the mixing component, which had been updated to address issues raised in the Swiss Post system with a similar mixing component.

Demtech raised five areas of concern and three recommendations.

The Demtech reviewers presented the detailed findings of their review to the NSW Electoral Commission including a discussion of risks and mitigations in the NSW Electoral Commission implementation, monitoring and procedures.

All issues raised from the source code review have been assessed by NSW Electoral Commission and additional testing or other work has been done to address them.

All recommendations made by Demtech have been adopted by the NSW Electoral Commission.

NSW Electoral Commission response to Demtech's report

This section is in alignment with the Demtech report. The section is written in the form of supplementary notes to both the report from Demtech (in Appendix A) and the document from Scytl (in Appendix B).

Executive summary

Demtech reported that the lack of major changes to the code since 2019 meant the risks were low, though highlighted that any risk from the recent minor changes "be mitigated through rigorous, systematic, and extensive testing". The NSW Electoral Commission has successfully completed the testing.

'Remaining areas of concern'	NSW Electoral Commission response
1. Remaining known vulnerabilities Demtech noted that "*the remaining vulnerabilities are carefully documented and accompanied by a rationale. Overall the rationales make sense*." Recommendation 1 relates to this.	The NSW Electoral Commission has also reviewed the remaining known vulnerabilities in the codebase and the rationales provided by Scytl, and concluded they present low risk and do not prevent using the software in the local government elections.
2. Trusted build issues Demtech noted the difficulty in being absolutely certain that the codebase reviewed matches the software that will be run for the election.	The current process gives NSW Electoral Commission sufficient confidence that the code being run matches the code reviewed. NSW Electoral Commission does intend to improve certainty that the codebase provided for future reviews matches the software build as Demtech suggest should be done after the local government elections in Recommendation 3, below.
3. Test quality Demtech raised concern over the quality of testing by Scytl, because only partial evidence of comprehensive testing was provided. Recommendation 2 relates to this.	NSW Electoral Commission agrees that there are opportunities to improve testing performed by Scytl, including 'fuzz testing' and test coverage reporting. Per recommendation 2, NSW Electoral Commission has mitigated risks for the local government elections by performing internal testing.
4. Documentation quality "The documentation of the iVote system is imprecise, incomplete, and in many parts out of date".	Scytl acknowledge this issue (Appendix B) and the NSW Electoral Commission will work with Scytl to improve documentation for future source code reviews, by adding explicit requirements to the contract.
5. Static code analysis Demtech raised concern over risk of concurrency problems if system has high usage. Recommendation 2 relates to this.	The NSW Electoral Commission has mitigated the risk of concurrency problems through extensive performance testing prior to the local government elections.

The NSW Electoral Commission fully accepts the Demtech recommendations as follows:

Demtech Recommendation	NSW Electoral Commission response
Recommendation 1 Demtech strongly recommended the vendor explanations for the remaining known CVEs be reviewed, so that the NSW Electoral Commission was satisfied with them and that any assumed mitigations were in place and sufficient.	The explanations provided by Scytl have been reviewed, together with the procedural, infrastructure or other mitigations in place, and the NSW Electoral Commission is satisfied with the results of this analysis.
Recommendation 2 Demtech strongly recommended reviewing the vendor test plans and ensuring NSW Electoral Commission testing covered any gaps and how the system behaved under high loads.	The NSW Electoral Commission has reviewed the Scytl test plans and our own, leading to an expansion of the performance testing completed by the NSW Electoral Commission. This testing has shown that the system is stable under loads much greater than expected for the local government elections.
Recommendation 3 An ongoing recommendation that after this election, the NSW Electoral Commission should implement a strategy to avoid future concerns over software maintenance. This would include on-site building of the system from the vendor source code and enhanced vendor maintenance of source code and documentation, plus monitoring of third-party libraries for security issues.	The NSW Electoral Commission agrees with the suggested improvements to code maintenance and build process and will work with Scytl to improve software quality processes, including more transparency of internal testing and review processes. This will be formalised by adding additional details to the contract requirements in early 2022.

Scope and review methodology

Demtech Statement/comment	NSW Electoral Commission commentary
Earlier code version 1.8	An initial version of source code provided by Scytl was deemed unacceptable due to extensive unused code libraries being included. Scytl was asked to remove unused libraries and provide a clean version for review. The source code reviewed in the Demtech report is 1.8.5. This is the version to be used for the 4 December elections, with the subsequent addition of 1 defect fix and correction of some instructional text for voters.

Functional matching

The review comments on documentation quality are noted, together with Scytl comments on the use of the Jira system as a repository for requirements.

Jira is a common industry platform, and its use should not prevent provision of adequate documentation to the source code reviewers. The NSW Electoral Commission will work with Scytl to determine how this issue can be addressed for future source code reviews.

Demtech Comments – Verifiability Analysis	NSW Electoral Commission commentary
3.2.1 Complexity	The NSW Electoral Commission will work with Scytl to ensure improvements made for the 1.8.5 version are continued, that complexity is reduced, and duplications eliminated.
3.2.2 Explicit erasure of votes	Covered in the corresponding section of Scytl's response (Appendix B).
3.2.3 Key generation and randomness	Covered in the corresponding section of Scytl's response (Appendix B).
3.2.4 Unused code	Noting Scytl's response to this item, the NSW Electoral Commission will discuss the options and risks to determine how to optimise removal of unused code while retaining the benefits of a software product (versus a bespoke system).
3.2.5 Missing contracts and invariants	The NSW Electoral Commission will discuss with Scytl the results of the coding guideline review and whether to add contracts to methods that define iVote.
3.2.6 Passwords	Covered in the corresponding section of Scytl's response (Appendix B).
3.2.7 Hardcoded passwords	Covered in the corresponding section of Scytl's response (Appendix B).
3.2.8 Quality of the specification	The NSW Electoral Commission will work with Scytl to improve the detail of their documents, as noted in response to Recommendation 3.

Static analysis

Demtech Comment	NSW Electoral Commission commentary
4.1 Trusted build	These are reflected in Recommendation 3 and are addressed in the response to that, above.
4.2 Analysis of SLOCcount Report	These are reflected in Recommendation 3 and are addressed in the response to that, above.

Demtech Comment	NSW Electoral Commission commentary
4.3 Analysis of Test Rail Report	These are reflected in Recommendation 3 and are addressed in the response to that, above.
4.4 SpotBugs Static Analysis	These are reflected in Recommendation 3 and are addressed in the response to that, above.

Attachment A – Demtech's Report

Published here https://www.elections.nsw.gov.au/About-us/Reports/iVote-reports

Attachment B – Scytl's Response

Published here https://www.elections.nsw.gov.au/About-us/Reports/iVote-reports