TECHNISCHE BESCHREIBUNG DES AUFGEDECKTEN FEHLERS UND LÖSUNG

Die Schweizerische Post hat den Quellcode ihres E-Voting-Systems am 7. Februar 2019 veröffentlicht. Seither gingen 67 Meldungen zum Code über den offiziellen Weg ein. Internationale IT-Experten fanden einen kritischen Fehler im Quellcode. Die Post hat ihren Technologiepartner Scytl aufgefordert, den Fehler umgehend zu korrigieren. Dies ist bereits erfolgt. Der angepasste Quellcode wird mit dem nächsten regulären Release zusammen mit einer aktualisierten Dokumentation veröffentlicht.

Um gleichzeitig das Stimmgeheimnis sowie die universelle Verifizierbarkeit zu garantieren, beruht das E-Voting-System der Post auf sogenannten verifizierbaren kryptographischen Misch-Netzwerken. Sie spielen eine wichtige Rolle, denn sie ermöglichen das Entkoppeln der Stimme vom Stimmbürger (Hintergrund-Artikel zur Rolle von Misch-Netzwerken im E-Voting). Das E-Voting-System der Post verwendet ein Bayer-Groth Misch-Netzwerk.

Das Bayer-Groth Misch-Netzwerk basiert auf kryptographischen Commitment-Verfahren, im konkreten Falle auf Pedersen-Commitments. Für Pedersen-Commitments werden zufällige und unabhängige Generatoren G und H benötigt. Der aktuell verwendete Algorithmus generiert diese Generatoren zwar zufällig. IT-Experten wiesen jedoch darauf hin, dass die Zufälligkeit und Unabhängigkeit der Generatoren im verwendeten Algorithmus nicht überprüft werden kann. Das Überprüfen der Zufälligkeit und Unabhängigkeit ist aber eine Voraussetzung für die Stichhaltigkeit der kryptographischen Beweise, auf denen die universelle Verifizierbarkeit des Systems beruht.

Auswirkung
Die universelle Verifizierbarkeit könnte während des Zählprozesses nicht sichergestellt sein, sodass potenzielle Manipulationsversuche nicht zweifelsfrei entdeckt werden könnten.

Um die Schwachstelle auszunutzen, müssten die Angreifer jedoch zahlreiche Schutzmassnahmen ausser Kraft setzen. Sie bräuchten beispielsweise Kontrolle über die gesicherte IT-Infrastruktur der Post sowie die Hilfe von mehreren Insidern mit Spezialwissen bei der Post oder den Kantonen.

Die Funktionsweise der individuellen Verifizierbarkeit ist vom aufgedeckten Fehler nicht betroffen. Die Systemversion, die aktuell in verschiedenen Kantonen im Einsatz ist, funktioniert somit gemäss den Anforderungen.

Lösung
Die Post hat den betroffenen Algorithmus bereits korrigieren lassen. Die Funktion, die die zufälligen Generatoren generiert, wurde mit einer verifizierbaren ausgetauscht, welche konform zum anerkannten Standard NIST FIPS 186-4 Appendix 2.3 ist. Das beschriebene Problem ist dadurch gelöst.

Die Anpassung wird die Post im nächsten regulären Quellcode-Release veröffentlichen zusammen mit weiteren Verbesserungen im Code, welche dank Feedbacks aus der Community umgesetzt werden konnten.

Experten, die den Fehler entdeckten
Der Fehler wurde von der folgenden Forschergruppe und Forschenden in dieser Reihenfolge eingereicht:

- Privacy & Anonymity Researcher Sarah Jamie Lewis (Open Privacy Research Society, Kanada); Professor Olivier Pereira (Université catholique de Louvain, Belgien); Associate Professor Vanessa Teague (The University of Melbourne, Australien)
- Forscher, der anonym bleiben möchte
- Prof. Dr. Rolf Haenni (Berner Fachhochschule, Schweiz)

Beobachtungen zum Quellcode sind willkommen
Interessierte Spezialisten haben weiterhin die Möglichkeit, den Quellcode des E-Voting-Systems der Post auf der Plattform GitLab einzusehen und Beobachtungen zu melden. Mehr Infos hier.

Werden Befunde gemeldet, gibt die Post den Spezialisten nach einer Analyse Feedback. Abschliessend analysierte Meldungen werden auf GitLab freigeschaltet, sofern die Einreicherin oder der Einreicher damit einverstanden ist. Abschliessend analysierte Meldungen zum Quellcode sind auf dem GitLab-Konto unter Issues ersichtlich (Zugang möglich nach Registration via www.post.ch/evoting-sourcecode).

Bis am 24. März 2019 findet zudem ein öffentlicher Intrusionstest am E-Voting-System statt. Mehr Infos hier.

Post CH AG
Entwicklung und Innovation
Wankdorfallee 4
Postfach
3030 Bern

evoting@post.ch
www.post.ch/evoting