# DESCRIZIONE TECNICA DELL'ERRORE RILEVATO E SOLUZIONE

Il 7 febbraio 2019 la Posta ha pubblicato il codice sorgente del suo sistema di voto elettronico. Nel frattempo sono giunte 67 segnalazioni ufficiali in merito. Gli esperti IT di tutto il mondo hanno trovato un errore critico nel codice sorgente. La Posta ha invitato il suo partner di tecnologia Scytl a correggere tempestivamente tale errore. La correzione è già avvenuta e il codice sorgente modificato verrà pubblicato in occasione della prossima release ordinaria unitamente a una documentazione aggiornata.

Al fine di garantire al contempo la segretezza del voto e la verificabilità universale, il sistema di voto elettronico della Posta si basa su cosiddette reti di mixaggio crittografiche verificabili. Quest'ultime svolgono un ruolo importante in quanto permettono di separare il voto dall'elettore (articolo di approfondimento sul (tedesco) ruolo delle reti di mixaggio nel voto elettronico, in tedesco). Il sistema di voto elettronico della Posta utilizza una rete di mixaggio Bayer-Groth.

La rete di mixaggio Bayer-Groth si basa su procedure di commitment crittografate, nello specifico su commitment Pedersen. Per i commitment Pedersen servono generatori G e H casuali e indipendenti. L'algoritmo utilizzato attualmente genera tali generatori in maniera casuale, ma gli esperti IT hanno fatto notare che non è possibile verificare la casualità e l'indipendenza dei generatori nell'algoritmo utilizzato. La verificabilità della casualità e dell'indipendenza è tuttavia un presupposto per la fondatezza delle prove crittografiche su cui si basa la verificabilità universale del sistema.

**Conseguenza**
La verificabilità universale potrebbe non essere garantita durante il processo di spoglio cosicché non sarebbe possibile individuare con certezza eventuali tentativi di manipolazione.

Tuttavia, per sfruttare questo punto debole gli hacker dovrebbero raggirare numerose misure di sicurezza. Ad esempio, dovrebbero avere il controllo dell'infrastruttura informatica protetta della Posta e aver bisogno dell'aiuto di diversi insider con conoscenze specifiche presso la Posta o i Cantoni.

La modalità di funzionamento della verificabilità individuale non è interessata dall'errore rilevato. La versione del sistema attualmente in uso in vari Cantoni funziona pertanto conformemente ai requisiti.

**Soluzione**
La Posta ha già fatto correggere l'algoritmo interessato. La funzione che genera i generatori casuali è stata sostituita con una funzione verificabile conforme allo standard riconosciuto NIST FIPS 186-4, appendice 2.3. Ciò permette di risolvere il problema di cui sopra.

La Posta pubblicherà l'adeguamento nell'ambito della prossima release ordinaria del codice sorgente unitamente ad altri miglioramenti nel codice apportati grazie agli input della community.

**Gli esperti che hanno scoperto l'errore**
L'errore è stato segnalato dai seguenti ricercatori in quest'ordine:

- Privacy & Anonymity Researcher Sarah Jamie Lewis (Open Privacy Research Society, Canada); Professor Olivier Pereira (Université catholique de Louvain, Belgio); Associate Professor Vanessa Teague (The University of Melbourne, Australia)
- Ricercatore che vuole rimanere anonimo
- Prof. Dr. Rolf Haenni (Berner Fachhochschule, Svizzera)

**Benaccette eventuali osservazioni sul codice sorgente**
Gli esperti interessati hanno tuttora la possibilità di visionare il codice sorgente del sistema di voto elettronico della Posta sulla piattaforma GitLab e di comunicare le loro osservazioni. Maggiori informazioni qui.

Se vengono comunicati dei risultati, la Posta procede ad analizzare tali risultati per poi fornire un riscontro agli specialisti. Le comunicazioni analizzate in maniera esaustiva vengono pubblicate su GitLab con il consenso dell'autore. Le comunicazioni sul codice sorgente analizzate in maniera esaustiva sono disponibili sull'account GitLab sotto Issues (è possibile accedervi dopo la registrazione tramite www.posta.ch/evoting-sourcecode).

Fino al 24 marzo 2019 è inoltre in corso un test pubblico di intrusione nel sistema di voto elettronico. Maggiori informazioni qui.

**Posta CH SA**
**Sviluppo e innovazione**
**Wankdorfallee 4**
**Casella postale**
**3030 Berna**

**E-mail: evoting@posta.ch**
**www.posta.ch/e-voting**