DESCRIPTION TECHNIQUE DE L'ERREUR DECELEE ET SOLUTION APPORTEE

Le 7 février dernier, la Poste a publié le code source de son système de vote électronique. Depuis, 67 messages relatifs au code ont été transmis par la voie officielle. Des experts en informatique d'envergure internationale ont décelé une erreur critique dans le code source. La Poste a demandé à son partenaire technologique Scytl de la corriger immédiatement. Le code source modifié sera publié avec le prochain release prévu et s'accompagnera d'une documentation réactualisée.

Pour pouvoir garantir à la fois le secret des urnes et la vérifiabilité universelle, le système de vote électronique de la Poste se fonde sur des «réseaux mixtes cryptographiques vérifiables». Ceux-ci jouent un rôle important en permettant le découplage du suffrage du votant (article de fond (en allemand) sur le rôle des réseaux mixtes dans le vote électronique). Le système de vote électronique de la Poste met en œuvre un réseau mixte Bayer-Groth.

Le réseau mixte Bayer-Groth se fonde sur une procédure de commitment cryptographique, en l'espèce sur des commitments Pedersen. Pour ces derniers, il faut avoir recours à des générateurs aléatoires et indépendants G et H. L'algorithme utilisé actuellement génère bel et bien ces générateurs sur un mode aléatoire, mais des experts informatiques font valoir le fait que le caractère aléatoire et indépendant des générateurs ne peut pas être vérifié dans l'algorithme utilisé. La vérification du caractère aléatoire et indépendant est toutefois une condition à remplir pour assurer la validité des preuves cryptographiques sur lesquelles se fonde la vérifiabilité universelle du système.

Conséquence
La vérifiabilité universelle pourrait ne pas être garantie pendant le processus de comptage de sorte que d'éventuelles tentatives de manipulation pourraient ne pas être décelées de manière indubitable.

Toutefois, pour exploiter la faille, il faudrait que les fraudeurs parviennent à invalider de nombreuses mesures de protection, par exemple en prenant le contrôle de l'infrastructure informatique sécurisée de la Poste et en bénéficiant de l'aide de plusieurs personnes détenant des connaissances spécifiques au sein de la Poste ou des cantons.

Le mode de fonctionnement de la vérifiabilité individuelle n'est pas concerné par l'erreur décelée. Par conséquent, la version du système qui est actuellement en usage dans différents cantons fonctionne conformément aux exigences.

Solution
La Poste a déjà fait corriger l'algorithme concerné. La fonction qui génère les générateurs aléatoires a été remplacée par une fonction vérifiable, qui est conforme au standard reconnu NIST FIPS 186-4, annexe 2.3. Le problème décrit est ainsi résolu.

La modification effectuée sera publiée par la Poste lors du prochain release du code source prévu, avec des améliorations complémentaires du code ayant pu être effectuées grâce aux retours d'information en provenance de la communauté.

Les experts qui ont décelé l'erreur
L'erreur a été découverte par le groupe de chercheurs et les chercheurs suivant de manière indépendante et dans cet ordre :

- Privacy & Anonymity Researcher Sarah Jamie Lewis (Open Privacy Research Society, Canada); Professor Olivier Pereira (Université catholique de Louvain, Belgique); Associate Professor Vanessa Teague (The University of Melbourne, Australie)
- Chercheur qui souhaite rester anonyme
- Prof. Dr. Rolf Haenni (Haute école spécialisée bernoise, Suisse)

LA POSTE

Toute observation relative au code source est la bienvenue
Les spécialistes intéressés ont toujours la possibilité de consulter le code source du système de vote électronique de la Poste sur la plateforme GitLab et de transmettre leurs observations. Informations complémentaires ici.

Dès lors que des éléments ont été décelés et signalés, la Poste fournit un feed-back après les avoir analysés. Une fois analysées de manière exhaustive, les observations communiquées sont mises en ligne sur GitLab pour autant que les personnes qui les ont transmises ne s'y opposent pas. Une fois analysées de manière exhaustive, les observations sur le code source peuvent être consultées sur le compte GitLab, à la rubrique «Issues» (accès possible après enregistrement via www.poste.ch/evoting-sourcecode).

Par ailleurs, le système de vote électronique est soumis à un test d'intrusion public jusqu'au 24 mars prochain. Informations complémentaires ici.

Poste CH SA
Développement et innovation
Wankdorfallee 4
Case postale
3030 Berne

evoting@poste.ch
www.poste.ch/evoting