Kanton St.Gallen Thurgau abraxas

22. August 2022

Die Staatskanzleien der Kantone Thurgau und St. Gallen teilen mit:

Expertinnen und Experten können Ergebnisermittlungssystem testen

Die Kantone Thurgau und St.Gallen haben ein neues Ergebnisermittlungssystem für Wahlen und Abstimmungen beschafft. Nachdem mehr als 140 IT-Expertinnen und -Experten das System intern auf Sicherheitslücken geprüft haben, folgt nun der zweite Schritt: Wer will, kann ab heute den ersten Teil des Quellcodes untersuchen und das System angreifen. Dank diesem öffentlichen Bug-Bounty-Programm wird das neue Ergebnisermittlungssystem noch sicherer.

Die Kantone Thurgau und St.Gallen lancieren das neue Ergebnisermittlungssystem für Wahlen und Abstimmungen nach dem Prinzip «Sicherheit durch Transparenz». Deshalb haben sie von der Anbieterin des Systems die Bereitschaft verlangt, den Quellcode offenzulegen, damit professionelle und private Security-Expertinnen und -Experten das System auf Herz und Nieren prüfen können.

Positive erste Erkenntnisse

Den ersten Schritt der Offenlegung startete die Abraxas Informatik AG am 23. Mai 2022 mit einem Private-Bug-Bounty-Programm. Mehr als 140 ausgewählte oder angemeldete Sicherheitsforscherinnen und Sicherheitsforscher konnten auf den Quellcode und die Dokumentation sowie das Ergebnisermittlungssystem in einer Vorabversion zugreifen und Angriffsversuche starten. Dank den Meldungen dieser «ethischen Hackerinnen und Hacker» konnte das System bereits verbessert werden.

Bis jetzt sind 28 Meldungen eingegangen. Davon wurden 14 als gültig bestätigte Sicherheitslücken im Rahmen des gesteckten Umfangs (Applikation Ergebnisermittlungssystem mit Berechtigungs- und Identitätenverwaltung) akzeptiert.

Eine davon wurde als hoch eingestuft, die anderen als tief oder mittel. 14'900 Franken an Prämien (Bountys) sind bisher ausbezahlt worden. Die bestätigten und korrigierten Meldungen sind auf der GitHub-Plattform mit dem Quellcode des Systems zu finden. Dazu wurde zu Beginn des Programms eine höhere Sicherheitslücke in der separaten Berechtigungs- und Identitätenverwaltung – dem Zugang zur Ergebnisermittlung – gemeldet. Es wurde nachträglich entschieden, diese Applikation in den Umfang des Auftrags aufzunehmen.

Start der öffentlichen Offenlegung

Ab heute Montag, 22. August 2022, wird das Programm in ein öffentliches Bug-Bounty-Programm überführt. Das bedeutet, dass private Security Researcherinnen und Researcher und alle interessierten Expertinnen und Experten ohne Anmeldung Teile des Codes und der Dokumentation einer Vorabversion des Systems einsehen und analysieren können. Es steht eine Testversion des Systems zur Verfügung, um Angriffsversuche starten zu können. Jede bestätigte gemeldete Sicherheitsschwachstelle wird belohnt. Dabei wird unter anderem die Auswirkung der Schwachstelle auf die Sicherheit des Systems und die Korrektheit der Ergebnisse berücksichtigt. Die Belohnung kann je nach Relevanz bis zu 30'000 Franken betragen.

Prinzip «Sicherheit durch Transparenz»

Durch die Offenlegung möchten die Kantone Thurgau und St.Gallen zu einer öffentlichen Debatte über die Sicherheit des neuen Ergebnisermittlungssystems beitragen. Durch die Offenlegung des Quellcodes und die Publikation der Schwachstellen und der Ergebnisse des Bug-Bounty-Programms ist für die Öffentlichkeit nachvollziehbar, dass die beiden Kantone und die Abraxas Informatik AG alles unternehmen, um die Sicherheit des neuen Ergebnisermittlungssystems auf dem aktuellen Stand zu halten. Die Offenlegung und das Bug-Bounty-Programm helfen dabei, Schwachstellen schnell zu finden und zu beheben. Ziel ist es, das neue System im kommenden Jahr einzusetzen. Wie oder wann genau das System eingesetzt wird, ist jedoch abhängig von den Ergebnissen der Offenlegung.

Weitere Informationen

Github-Plattform mit dem Quellcode des Systems

Informationen über das öffentliche Bug-Bounty-Programm:

- abraxas.ch/bugbounty
- bugbounty.ch/abraxas

Ergebnisermittlungssystem (tg.ch)

Ergebnisermittlungssystem (sg.ch)

Medienmitteilung vom 23.05.2022 (sg.ch)

Medienmitteilung vom 23.05.2022 (tg.ch)

Medienauskunft:

Abraxas Informatik AG: gregor.patorski@abraxas.ch

Kanton St.Gallen: kommunikation@sg.ch

Kanton Thurgau: medien.sk@tg.ch