3. januar 2024

Oppfølgning av kildekoderevisjon utført av mnemonic

Valgdirektoratet gjennomfører rutinemessig eksterne kildekoderevisjoner som en del av direktoratets systemforvaltning. I forbindelse med oppdraget som direktoratet har fått med å utvikle en digital løsning for de konkrete folkeavstemningene i områdene som tidligere utgjorde Søgne og Songdalen kommune, har mnemonic fått i oppgave med å gjennomføre kildekoderevisjonen.

Revisjonen ble utført i månedsskiftet november 2023, og omfattet all kildekode til løsningen for folkeavstemninger.

Målet med revisjonen er å få en uavhengig vurdering av kildekode og systemarkitektur, med vekt på sikkerhet og kvalitet. Sikkerhet forstås som feil eller mangler i applikasjonskode og/eller arkitektur som i utilstrekkelig grad utelukker tredjeparts manipulasjon av løsningen (integritet, tilgjengelighet og konfidensialitet). Kvalitet forstås som feil eller mangler i kode som påvirker kodekompleksitet, kodeorganisering og bruk av kodebibliotek/rammeverk som kan gjøre det vanskelig å forstå, vedlikeholde og teste koden.

Mnemonic klassifiserer sine funn fra 4-critical til 1-low og har i tillegg en kategori 0-info, og anbefaler oppfølging basert på klassifiseringen slik:

- Critical findings are “showstoppers” that mnemonic thinks should be subject to immediate/emergency remediation, based on their potential impact.
- High-severity findings should normally be prioritized for analysis and possible remediation within an urgent time-frame.
- Medium-severity findings should be subject to remediation following usual vulnerability management and triage processes.
- Low-severity findings should be subject to remediation following usual vulnerability management and triage processes, but the initial evaluation is that they may be of lower priority.
- Informational findings should be reviewed by relevant stakeholders.

1.1 Funn

Tabellen under viser antall funn i og Mnemonics klassifisering av funnene

Modul	Funn fordelt på klassifisering				
	Critical	High	Medium	Low	Info
Folkeavstemning	1	0	3	2	4

1.2 Oppfølgning

Funnene blir fulgt opp slik:

4 – Critical:	Ble avdekket av direktoratet samtidig som mnemonic. Konfigurasjonsfeil som ble oppdaget ved testing.
3 – High:	Ingen funn.

2 – Medium:	Alle funn er enten utført eller vurdert som ikke nødvendig. Beskrivelse av vurderinger: Recommendation 2: utført. Recommendation 3: ikke utført. Funnet krever at angriperen allerede har tilgang på innsiden. Recommendation 4: ikke aktuell. Vi har alltid benyttet to nøkler for signering og dekryptering.
1 – Low:	Alle funn er enten utført eller vurdert som ikke nødvendig. Beskrivelse av vurderinger: Recommendation 5: utført. Ugyldig data gir statusen <UGYLDIG STEMME>. Recommendation 6: utført. Ugyldig data gir statusen <UGYLDIG STEMME>.
0 – Info:	Alle funn er enten utført eller vurdert som ikke nødvendig. Beskrivelse av vurderinger: Recommendation 7: ikke utført. Funnet krever at angriperen allerede har tilgang på databasen. Recommendation 8: utført. Vi logger når velger får kryss i manntallet. Recommendation 9: ikke aktuell. Endringer i bruksområdet for manntallsnummer har gjort at vi har gått tilbake til sekvensielle tall. Recommendation 10: ikke utført. Standarden krever kryptografiske funksjoner som ikke er støttet i nettlesere enda (RSAVP1 og EMSA-PSS-ENCODE). Selv om det kunne vært støttet i noen nettlesere, vil det skape problemer hvis velger bruker eldre nettlesere.

Vedlegg

Mnemonics rapport fra kildekoderevisjon av folkeavstemning

- Valgdirektoratet – Folkeavstemning Source Code Review v1. 0 1.pdf