Exclusions

Author	Abraxas Informatik AG
Classification	public
Version	2.2
Date	19. Aug 2022

abraxas

Known Security Issues VOTING IAM / VOTING Ausmittlung

ID	Title	Summary
VOTING-1405	Input validation VOTING Ausmittlung	The interface definitions can be found here: https://github.com/abraxas-labs/voting-ausmittlung-proto/blob/main/docs/api-specs/ The implementation is currently pending.
VOTING-1805	Extend file upload with check for MIME type / file extension	The uploaded files are not validated against a set of criteria (extension, content type, magic bytes).
VOTING-1806	PostGres DB - User Management	The postgres database access does not fulfill least privilege principle.
VOTING-1913	DmDoc - disallow username in URL	The DmDoc service api uses sensitive username data as part of the requesting url.
VOTING-2023	Transient Subscription failures Health State	A failure during the replay of transient catch-up subscription potentially leads into infinitely retries.
SEC-537	Confirmation mail to old address in case of change of e-mail address	Insecure eMail change process needs to be improved
SEC-565	2FA replace flow	Current 2FA replacement process does not force a confirmation with old 2FA
SEC-605	Auth request key (URL param) additionally secured with session cookie	In addition to Request ID in URL a session cookie for the authentication flow needs to be introduced
SEC-639	Client Refresh Flow Implementation	The IAM service is going to introduce OAuth2 refresh tokens with revocation. VOTING Ausmittlung will improve its session handling using refresh tokens as soon as the IAM is ready.
SEC-687	Client-side logout,	Implement proper client side logout with invalidating the session cookie on server side
SEC-689	Token Binding & Token Revocation	Token binding and token revocation is not supported by the IAM service. Therefore, it is not implemented for VOTING Ausmittlung.