Exclusions

Author	Abraxas Informatik AG
Classification	public
Version	2.4
Date	27. Sept 2022

For digital Switzerland. For Sure.

abraxas

Known Security Issues VOTING IAM / VOTING Ausmittlung

ID	Title	Summary
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.
VOTING-2226	Protect event processor against replay attacks	An attacker can repeat correctly signed events unnoticed and thus manipulate the data under certain circumstances.
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	Refresh Token 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	The Session handling on the IAM is going to be improved by introducing proper invalidation of the session cookie and revocation of OAuth2 tokens on a logout.