PER Auskunft

Exclusions

Author	Abraxas Informatik AG
Classification	public
Version	1.0
Date	11. October 2024

Known Security Issues PER Auskunft

ID	Title	Summary
PERREGIST-5369	Authorization Code GET Params	The OpenID Authorization Code is sent to the client as a GET parameter instead of a POST payload.

Known Security Issues IAM System of PER Auskunft

The IAM system used in the Bug Bounty program for the product "PER Auskunft" includes specific PRE-production configurations, which may differ in some aspects from those in production. These elements are also included in the list below:

ID	Title	Summary
SEC-1610	Activated third-party IDP's	Third-party IDPs are activated on the PRE environment for test purposes only.
SEC-1490	Activated FeatureFlag AlwaysAllowedRedirectUris	The PRE environment contains a global redirect URI whitelist, which contains specific domains, independent of application-specific configurations.
SEC-1159 SEC-823	Token lifetime	A token lifetime of 24 hours is configured on the PRE environment.
SEC-919 SEC-823	RememberMe and cookie lifetime	A RememberMe and cookie lifetime of 1 week is configured on the PRE environment.
Misc.	Feature configurations	For test reasons, the following FeatureFlags are deactivated on the PRE environment: - PreventAccountDowngrade (2FA) - SecurityNotificationsEnabled - EnableImmutableFields - EnforceAnyRoleOnAuthorization