3339155 - OData APIs – Wrong usage of session cookies

Component: LOD-CRM-INT-API (OData API (C4C Only)), Version: 4, Released On: 07.08.2023

Symptom

What is the change?

Before: Security sessions were created and the CSRF token was bound to the security session. If the calls were made without sending the cookies back to server, new security sessions were getting created with every call and it decreased performance of OData calls.

Now: No security sessions are created but for the Cross-Site Request Forgery (CSRF/XSRF) protection a dedicated cookie is set.

Environment

SAP Cloud for Customer

SAP Business ByDesign

Cause

Why the change?

We observed performance degradation during high ODATA activity due to very high number of security sessions being created. This change is implemented to optimize the performance by optimizing security session handling.

Resolution

What is the impact?

Integration scenarios using ODATA APIs might be impacted if not all cookies are sent back to server in subsequent OData calls. The impact is especially seen when "x-csrf-token" value is sent via request header along with a specific session cookie (instead of all cookies).

In such cases, CSRF token validation fails resulting in HTTP response code: 403 - Forbidden.

Example Change observed?

Before Change: Cookie with name: SAP_SESSIONID_<SID>_<Tenant Internal ID> was sent in the response from the server which was utilized by the customers/partners for the ODATA calls.

After Change: Cookie with name: SAP_SESSION_<SID>_<Tenant Internal ID> is not returned in response header by server. Cookie with name sap-XSRF_<SID>_<Tenant Internal ID> is returned in the server response only when "x-csrf-token" is sent in the request header.

If "x-csrf-token" not requested, cookie "sap-XSRF_<SID>_<Tenant Internal ID>" is not returned.

Expectation from Customer?

Clients should not have any validations or checks or any kind of coding based on cookie names. Such checks need to be removed and the behaviour should be tested.

Clients consuming OData services should send back all cookies received from the server in subsequent calls to that server (without any filtering on cookie names).

How to Test?

OData API calls should work as it used to work earlier, before and after the change is applied in the system.

Products

Products
SAP Business ByDesign all versions
SAP Cloud for Customer core applications all versions