VULNERABILITY REPORT

APIsec Security Assessment

Scan ID:	019a507c-819d-73ce-8851-2d3dc6376e22
Status:	Complete
Generated:	November 25, 2025 at 06:08 PM

Executive Summary

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	2	2	0

Scan Statistics

Endpoints Scanned: 1 / 1
Total Tests: 99
Tests Passed: 95

Tests Failed: 1
Total Findings: 4
Endpoints Affected: 1

Findings

/ext-services2/central/tpp-rdmp/operational-risk-models/customer-risk-profile/get ...

incremental

MEDIUM

Endpoint: post /ext-services2/central/tpp-rdmp/operational-risk-models/customer-ri...
Category: idor
CVSS Score: 5.0
OWASP: API1:2023

This test looks for object identifiers that are incremental IDs. An incremental identifier is an identifier that increments in value in a predictable way. Currently, the test does this by checking if the identifier is numerical.
The test analyzes response payloads and searches them for fields that look like IDs. The heuristic used for this analysis looks for fields with the following patterns:
... [see full report]

HTTP Request:

```
post https://partner-api-sit.bmo.com/ext-services2/central/tpp-rdmp/operational-risk-models/customer-risk-profile/get
x-request-id: g4565-78sdf9-56s98
Authorization: Bearer eyJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJhcGkyLXNpdDIuYm1vZ2MubmV0Iiwic3ViIjoiYW5vbnltb3VzIiwiZXhwI
joxNzY0ODc2ODgyLCJpYXQiOjE3NjIyODQ4ODIsInNjb3BlIjoidmVuZG9yLXNlYy1kZXYtcmVzb3VyY2VzZXJ2ZXIvdHBwLXJkbXA
ub3BlcmF0aW9uYWwtcmlzay1tb2RlbHMuY3VzdG9tZXItcmlzay1wcm9maWxlLnJlYWQifQ.AN_D3qyxG9YHh72WaTzgYH0hVnbM
lCBpF9Qztagjmc5is-DUHVHByOQ4Gicv63kaBSD8fBuyuNmI3dPAG5hN8Y6XNXdhYOUhkhv2ysxMV81ETTNCYXV_RxlNUik7aUZ
V19FW3eS5iYKDmjKX90N8M8M2geyCl_X5UDATp9IQ499CdZgw6CYSmyIuD-eviUsCcARY_w8yYmwe2T1AkGrZyobo0LFrmhcGC
LPWgJcBUUl8HQgzMpKP9g9OTtgnht3zvbQH18viuIt3pjv4pS_aGgbjcHy3RlN9YjAqm_FWE9_EOtWcw8ZvkBQ3RZ2a0FK9PIfe8tZ
X_mZUZEgDQnickw
x-fapi-interaction-id: 12345
x-fapi-financial-id: 001
x-app-cat-id: 85695
x-api-key: dee4f13e03a36cd6ed584e8f0bdc1fdc
content-type: application/json

... [truncated]
```

HTTP Response (200):

```
HTTP 200
x-request-id: g4565-78sdf9-56s98
x-global-transaction-id: e873bc6b690a5d5214f1c170
date: Tue, 04 Nov 2025 20:08:51 GMT
server: Server
x-amz-apigw-id: TiOE6HiN4osFoLw=
x-backside-transport: OK OK
x-amzn-requestid: c6fb0bd9-0721-4a88-af91-dce909bd6f1a
vary: Accept-Encoding
x-ratelimit-limit: name=default,100;
x-request-time: 1762286931209
x-ratelimit-remaining: name=default,84;
strict-transport-security: max-age=63072000 ; includeSubDomains ; preload
x-amzn-trace-id: Root=1-690a5d52-65df7fa97c992ad2e6f5918d
connection: keep-alive
... [truncated]
```

cors

MEDIUM

Endpoint: post /ext-services2/central/tpp-rdmp/operational-risk-models/customer-ri...
Category: headers
CVSS Score: 5.0
OWASP: API8:2023

This test checks whether your site uses a cross-origin resource sharing (CORS) policy, and if it does, whether your CORS policy is securely configured.

By default, browsers do not allow cross-origin requests, however this feature can be enabled by including the
... [see full report]

rateLimit

LOW

Endpoint: post /ext-services2/central/tpp-rdmp/operational-risk-models/customer-ri...
Category: headers
CVSS Score: 3.0
OWASP: API8:2023, API4:2023

This test checks whether the API includes the RateLimit header in the responses. If responses don't contain a rate limiting header, the test raises an informational detection.
It's best practice to implement rate-limiting policies for APIs, and to document those policies using the RateLimit header. The RateLimit header makes it clear for API consumers how often they can call the API, hence avoiding accidental misuse of the API.
... [see full report]

jwt_conformance

LOW

Endpoint: post /ext-services2/central/tpp-rdmp/operational-risk-models/customer-ri...
Category: token
CVSS Score: 1.0
OWASP: API2:2023

This test checks whether your JSON Web Tokens (JWTs) implement the standard specification. We test this by checking for the presence of the JWT registered claims from [RFC 7915](https://datatracker.ietf.org/doc/html/rfc7519):

- iss: the issuer of the token.

... [see full report]