

[generiekzaakafhandelcomponent](#) / [gzac-issues](#) Public[Code](#) [Issues](#) 288 [Pull requests](#) [Actions](#) [Projects](#) [Wiki](#) [Security](#)[New issue](#)

Inbox & SSE event mapper: sensitive data logging, silent exceptions, and null safety issues #653

ClosedBug

Assignees



Labels

CommUtrsecurity

Milestone

13.22.0

theo-ritense opened 3 weeks ago

Collaborator

Affected version

Current (next-minor)

Expected behavior

1. **InboxHandlingService** must not log full message payloads to stdout. These payloads may contain sensitive data (user IDs, roles, result data) and it is unknown who has access to the application logs. Sensitive data should never be written to stdout.
2. **ValtimoCloudEventMapper** should log errors when CloudEvent deserialization or mapping fails, so developers can diagnose issues (without logging the sensitive payload).
3. **DocumentSseEventMapper** should gracefully handle a null `resultId` for `DocumentUpdated` events instead of throwing a `NullPointerException`.
4. **ConfigurationIssueSseEventMapper** should not send a `ConfigurationIssueUpdatedSseEvent` when both `caseDefinitionKey` and `caseDefinitionVersionTag` are null/empty, as such an event carries no useful information.

Current behavior

1. `InboxHandlingService.handle()` logs the full message payload at INFO level (`inbox/src/main/kotlin/com/ritense/inbox/InboxHandlingService.kt:25`):

```
logger.info("Received message: {}", message)
```



2. ValtimoCloudEventManager.fromJson() and toValtimoEvent() catch all exceptions and return null without any logging (inbox/src/main/kotlin/com/ritense/inbox/ValtimoCloudEventManager.kt:33-57):


```
} catch (ex: Exception) {
    null
}
```
3. DocumentSseEventManager uses !! on event.resultId, which throws a KotlinNullPointerException if null (case/src/main/kotlin/com/ritense/document/mapper/DocumentSseEventManager.kt:40):


```
DocumentUpdatedSseEvent(it.resultId!!)
```
4. ConfigurationIssueSseEventManager falls back to ?: "" for caseDefinitionVersionTag, producing a meaningless event (case/src/main/kotlin/com/ritense/case/mapper/ConfigurationIssueSseEventManager.kt:36):


```
caseDefinitionVersionTag = result?.get("caseDefinitionVersionTag")?.asText() ?: ""
```

Possible solution

1. Change log level to debug and remove the payload: `logger.debug { "Received inbox message" }`
2. Add warning-level logging in the catch blocks (without the raw payload):


```
} catch (ex: Exception) {
    logger.warn(ex) { "Failed to deserialize CloudEvent" }
    null
}
```
3. Return null when resultId is null:


```
DocumentUpdated.TYPE -> {
    val resultId = event.resultId ?: return null
    DocumentUpdatedSseEvent(resultId)
}
```
4. Return null when caseDefinitionVersionTag is missing:


```
val caseDefinitionVersionTag = result?.get("caseDefinitionVersionTag")?.asText()
?: return null
```

Steps to reproduce

1. Send a message through the inbox — observe that the full payload is logged at INFO
2. Send a malformed message through the inbox — it is silently dropped with no log output
3. Publish a DocumentUpdated event without a resultId — a KotlinNullPointerException is thrown
4. Trigger a ConfigurationIssueUpdated event without a caseDefinitionVersionTag — a meaningless event with an empty version tag is dispatched



theo-ritense assigned [ThomasMinkeRitense](#) 3 weeks ago



elenacherneenkova 3 weeks ago

Collaborator



Bedankt voor het melden van dit probleem. We zullen de onderliggende oorzaak onderzoeken en je informeren zodra duidelijk is wanneer de oplossing kan worden geleverd.

Mocht er tijdens het onderzoek aanvullende informatie van jouw kant nodig zijn, dan nemen we contact met je op.

elenacherneenkova added this to [GZAC](#) 3 weeks agoelenacherneenkova added the **Bug** issue type 3 weeks agoelenacherneenkova added **CommUtr** 3 weeks agoelenacherneenkova moved this to TO DO in [GZAC](#) 3 weeks agoKlaas-Ritense moved this from TO DO to IN PROGRESS in [GZAC](#) 3 weeks agoKlaas-Ritense assigned [Klaas-Ritense](#) and unassigned [ThomasMinkeRitense](#) 3 weeks ago

Klaas-Ritense mentioned this 3 weeks ago

[GH-653: Fix sensitive data logging, etc valtimo-platform/valtimo#497](#)Klaas-Ritense added this to the [13.22.0](#) milestone 3 weeks agotheo-ritense added **security** 3 weeks agoelenacherneenkova closed this as [completed](#) 2 weeks agoelenacherneenkova moved this from IN PROGRESS to DONE in [GZAC](#) 2 weeks ago

Sign up for free

to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

Metadata

Assignees



Klaas-Ritense

Labels

CommUtr

security

Type

Bug

Projects

 GZAC

Status

DONE



Milestone

 13.22.0

Closed 2 weeks ago, 100% complete

Relationships

None yet

Development

No branches or pull requests

Participants

