Sensitive data exposure through inbox message logging in InboxHandlingService

Moderate **theo-ritense** published **GHSA-hfrg-mcvw-8mch** 2 days ago

Package

com.ritense.valtimo:inbox (Maven)

Affected versions

>= 13.0.0, < 13.22.0

Patched versions

13.22.0

Description

Summary

The `InboxHandlingService` logs the full content of every incoming inbox message at INFO level (`logger.info("Received message: {}", message)`). Inbox messages are wrappers around outbox message data, which can contain highly sensitive information such as personal data (PII), citizen identifiers (BSN), and case details.

Impact

This data is exposed to:

- Anyone with access to application logs (stdout/log files)
- Any Valtimo user with the admin role, through the logging module in the Admin UI

Affected Code

`com.ritense.inbox.InboxHandlingService#handle` in the `inbox` module.

Resolution

Fixed in 13.22.0 via commit `f16a1940ba` (PR #497, tracking issue gzac-issues#653). The log statement was downgraded from INFO to DEBUG and the message payload was removed from the log output.

Mitigation

For versions before 13.22.0, consider:

- Restricting access to application logs
- Adjusting the log level for `com.ritense.inbox` to WARN or higher in your application configuration

Severity

Moderate 4.9 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	Low
Privileges required	High
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	None
Availability	None

Learn more about base metrics

CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N

CVE ID

CVE-2026-34164

Weaknesses

▶ CWE-532