Release notes 3.9.8

Summary: Version 3.9.8 of Eclipse Ditto, released on 08.10.2026

Table of Contents

- Changelog
  - Security fixes
    - Security fix for CVE-2026-107503 — Session takeover via the Ditto UI `environmentsURL` query parameter
  - Changes
    - Dependency updates fixing known vulnerabilities
  - Bugfixes
    - Fix MQTT messages getting lost right after a connection was (re)established
    - Fix `put-metadata` nesting deeper on consecutive modifications
    - Return HTTP 401 instead of 503 for JWTs missing the `iss` or `kid` claim
    - Fix HTTP 500 when deleting a Feature not defined in the WoT ThingModel
    - Fix log placeholders and dropped exception causes
    - Make the Ditto UI OIDC silent token refresh work
  - Helm Chart
- Migration notes

Edit this page

This is a **security bugfix release**, no new user-facing API features since 3.9.7 (release_notes_397.html) were added. It fixes a security vulnerability in the Ditto UI (and the Swagger UI OIDC integration) which allowed a crafted link to take over a user's login session, updates dependencies with known vulnerabilities and contains several bugfixes in the things, gateway and connectivity services — among them MQTT messages getting lost right after a connection was (re)established.

Note: We recommend all users of the Ditto UI or the Swagger UI with SSO (OIDC) login to update to this release. See the *Security fixes* section below for the exact preconditions and for workarounds if you cannot upgrade immediately.

Changelog

Compared to the latest release 3.9.7 (release_notes_397.html), the following security fixes, changes and bugfixes were added.

Security fixes

The vulnerability was reported and fixed privately, and is disclosed through the GitHub Security Advisory process. As the fix was merged from a private fork, there is no public pull request for it; the fix commit is linked directly instead. The linked advisory carries the full details, including the affected code, the fix and the available workarounds.

Security fix for CVE-2026-107503 — Session takeover via the Ditto UI `environmentsURL` query parameter

Advisory GHSA-8767-g5qv-9jcf / CVE CVE-2026-107503 / Fix commit `d4e51ba20e`

Severity **high** (CVSS 4.0 score 7.1, `CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:A/VC:H/VI:L/VA:N/SC:H/SI:H/SA:N`).

The Ditto UI (user-interface.html) can load its environments — including the Ditto API URI and the OIDC (SSO) provider configuration — from a JSON file referenced by the `environmentsURL` query parameter. Affected versions fetched this file from **any URL**, adopted it without user confirmation and persisted it in the browser's local storage (CWE-15, CWE-346).

A crafted link to a Ditto UI deployment could therefore configure an attacker-controlled OIDC `authority` with automatic SSO enabled. The UI then started a login at the genuine identity provider, but exchanged the returned authorization code — together with its PKCE `code_verifier` — at an attacker-controlled token endpoint, allowing the attacker to redeem it for the user's access and refresh tokens (CWE-522). Alternatively, an attacker-controlled `api_uri` made the UI send the user's bearer token or Basic credentials to the attacker. As the injected environment was persisted, later visits of the UI without the crafted link repeated the attack.

Affected are Ditto UI versions **3.6.0 through 3.9.7** (including the hosted instance at eclipse-ditto.github.io/ditto/), when an OIDC client at the identity provider registered the UI's URL as `redirect_uri`. The Swagger UI OIDC integration of the Helm chart and the Docker Compose deployment (since **3.9.0**) read the OIDC provider configuration via the same `environmentsURL` parameter and were affected as well, but only after the user actively started a login via "Authorize".

The Ditto UI and the Swagger UI now only load environments via `environmentsURL`:

- from the **same origin** the UI is served from,
- never from paths containing `/api/` or `/ws/` — below which a Ditto deployment serves JSON written by its users, e.g. Thing attributes, which would otherwise allow users to craft environments for other users,
- only via `http` or `https` (e.g. no `data:` URLs), also re-validating the target of redirects.

Environments may additionally be loaded from origins configured in an optional `ui-config.json` file served next to the UI — see Restrictions for`environmentsURL` (user-interface.html#restrictions-for-environmentsurl). Only add origins whose content is fully trusted.

If you cannot upgrade immediately, do not open Ditto UI or Swagger UI links containing an `environmentsURL` parameter from untrusted sources. If you may have opened such a link, remove the environments stored in your browser (via the UI's "Environments" tab or by clearing the site data of the UI) and log out from your identity provider in order to revoke the potentially leaked sessions.

Changes

This is a complete list of the merged pull requests.

Dependency updates fixing known vulnerabilities

PR #2548 updates `netty-handler`, fixing CVE-2026-62243, CVE-2026-75596 and CVE-2026-75595, and `httpclient5` (a transitive dependency of the AWS SDK), fixing CVE-2026-71290.

Bugfixes

Fix MQTT messages getting lost right after a connection was (re)established

PR #2562 fixes MQTT messages received by an MQTT connection (connectivity-protocol-bindings-mqtt5.html) right after it was established or re-established being lost — for all MQTT versions. The connectivity service stopped buffering incoming messages before the consumers had actually subscribed to them, so a message arriving in that (usually sub-millisecond) window was dropped and never acknowledged to the broker, even with QoS 1 or 2. Buffering is now only stopped once all consumers confirmed their subscription. The MQTT protocol exchange with the broker is unchanged.

Fix `put-metadata` nesting deeper on consecutive modifications

Issue #2568 / PR #2569 fixes metadata (basic-metadata.html) set via the `put-metadata` header being nested recursively deeper with every consecutive `PUT` of a Feature property or `ModifyFeature` command, instead of being updated at the targeted path. The metadata was built relative to the command's resource path and then applied at that path again, duplicating the path in the stored `_metadata`.

Return HTTP 401 instead of 503 for JWTs missing the `iss` or `kid` claim

PR #2567 fixes the gateway answering a syntactically valid JWT which lacks the mandatory `iss` and/or `kid` claim with HTTP 503 `gateway:authentication.provider.unavailable` instead of HTTP 401. This reported a client-side authentication failure as a server-side outage and inflated 5xx error metrics and alerting. Genuine unavailability of the OpenID Connect provider is still answered with 503.

Fix HTTP 500 when deleting a Feature not defined in the WoT ThingModel

PR #2545 fixes deleting a Feature which is not defined in the Thing's WoT ThingModel (basic-wot-integration.html) failing with HTTP 500 when WoT validation is enabled. Such deletions now succeed.

Fix log placeholders and dropped exception causes

PR #2578 fixes several log and error messages — mainly in the connectivity service — using placeholder syntax not matching the logger they were passed to, so that their arguments were never substituted. Connection logs, for example, showed a literal `{}` instead of the cause of a failed publish, and some errors were logged without their exception message and stack trace.

Make the Ditto UI OIDC silent token refresh work

PR #2549 fixes the Ditto UI's `silent-callback.html` page, used for refreshing OIDC tokens in a hidden iframe when no refresh token is available. The page was never included in the `eclipse/ditto-ui` Docker image and could not have run even when served, so silent token refresh without a refresh token never worked.

Helm Chart

The Helm chart was updated to version `4.8.0`, bumping the Ditto `appVersion` to `3.9.8`.

As part of the security fix, it adds the `dittoui.environmentsURL.allowedOrigins` value (default `[]`). It is rendered into a new `<release>-ui-config` ConfigMap, which is mounted as `ui-config.json` into both the Ditto UI and the Swagger UI and configures additional origins the UIs may load environments from via `environmentsURL`. Only add fully trusted origins — `"*"` accepts any origin and makes the UIs vulnerable again.

It also contains the fix planned for the never released chart version `4.7.1`: PR #2540 fixes `thingsSearch.config.customIndexes` never reaching Ditto, as the chart rendered it at a config path the things-search service does not read. Worse, as things-search drops all indexes on startup which are neither built-in nor configured, custom indexes declared via the chart — or created manually — were **dropped** instead of being created and kept.

The full, itemized list of chart changes lives in the chart's own CHANGELOG.

Migration notes

There are no migration steps required for the Ditto data model or APIs.

However, the fix for CVE-2026-107503 changes the behaviour of the `environmentsURL` query parameter of the Ditto UI and the Swagger UI: **environments are only loaded from the UI's own origin.** Links pointing `environmentsURL` to a file on another origin now fail with an error message, and the UI falls back to the environments stored in the browser.

Deployments which intentionally serve their environments file from another origin must either serve it from the UI's own origin (e.g. `https://<ditto-hostname>/ui-environments.json`), or allow that origin via a `ui-config.json` file served next to the UI:

```
{
  "environmentsURL": {
    "allowedOrigins": ["https://config.example.com"]
  }
}
```

When deploying with the Helm chart, configure this via the `dittoui.environmentsURL.allowedOrigins` value. Users of the hosted Ditto UI at eclipse-ditto.github.io/ditto/ can no longer load environments from other origins via `environmentsURL`; they can still create or paste environments in the UI's "Environments" tab.

Tags: release_notes (tag_release_notes.html)