Release notes 3.8.14

Summary: Version 3.8.14 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
    - Helm Chart
- Migration notes

Edit this page

This is a **security bugfix release** for the 3.8 line, no new features since 3.8.13 (release_notes_3813.html) were added. It contains **only** the fix for the security vulnerability also fixed in 3.9.8 (release_notes_398.html) — a session takeover via the Ditto UI's `environmentsURL` query parameter — and dependency updates fixing known vulnerabilities, but no other changes.

Note: We recommend all users of the Ditto UI of the 3.8 line 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. Users who can upgrade to the 3.9 line should prefer 3.9.8 or later.

Changelog

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 advisory is linked instead and 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

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.

On the 3.8 line, all versions up to and including 3.8.13 are affected (the OIDC login of the Ditto UI exists since 3.6.0 (release_notes_360.html)), when an OIDC client at the identity provider registered the URL of the deployed Ditto UI as `redirect_uri`. The Swagger UI OIDC integration, which is affected in the 3.9 line, does not exist in 3.8.

The Ditto UI now only loads 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 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

Dependency updates fixing known vulnerabilities

The dependency updates of PR #2548 were backported: `netty` was updated from `4.2.4.Final` to `4.2.17.Final`, fixing CVE-2026-62243, CVE-2026-75596 and CVE-2026-75595, and the AWS SDK (used for MongoDB AWS IAM authentication) from `2.33.0` to `2.54.9`, which updates its transitive `httpclient5` dependency fixing CVE-2026-71290.

Helm Chart

The Helm chart was updated to version `3.8.14`, bumping the Ditto `appVersion` to `3.8.14`.

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 the Ditto UI and configures additional origins the UI may load environments from via `environmentsURL`. Only add fully trusted origins — `"*"` accepts any origin and makes the UI vulnerable again. There are no other chart changes.

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: **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.

Tags: release_notes (tag_release_notes.html)