SQL injection via forged pagination tokens

High **zepatrik** published **GHSA-hgx2-28f8-6g2r** 2 weeks ago

Package

github.com/ory/kratos (Go)

Affected versions

v25.4.0

Patched versions

v26.2.0

Description

Description

The **ListCourierMessages** Admin API in Ory Kratos is vulnerable to SQL injection due to flaws in its pagination implementation.

Pagination tokens are encrypted using the secret configured in `secrets.pagination`. An attacker who knows this secret can craft their own tokens, including malicious tokens that lead to SQL injection. If this configuration value is not set, Kratos falls back to a default pagination encryption secret. Because this default value is publicly known, attackers can generate valid and malicious pagination tokens manually for installations where this secret is not set.

Preconditions

This issue can be exploited when the following conditions are met:

- **ListCourierMessages API** is directly or indirectly accessible to the attacker
- The attacker can pass a raw pagination token to the affected API
- The configuration value `secrets.pagination` is not set or known to the attacker

Impact

An attacker can execute arbitrary SQL queries through forged pagination tokens.

Mitigation

As a first line of defense, **immediately** configure a custom value for `secrets.pagination` by generating a cryptographically secure random secret, for example:

```
openssl rand -base64 32
```

Next, upgrade **Kratos** to a fixed version **as soon as possible**.

Severity

High 7.2 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-33503

Weaknesses

▶ CWE-89