BACK

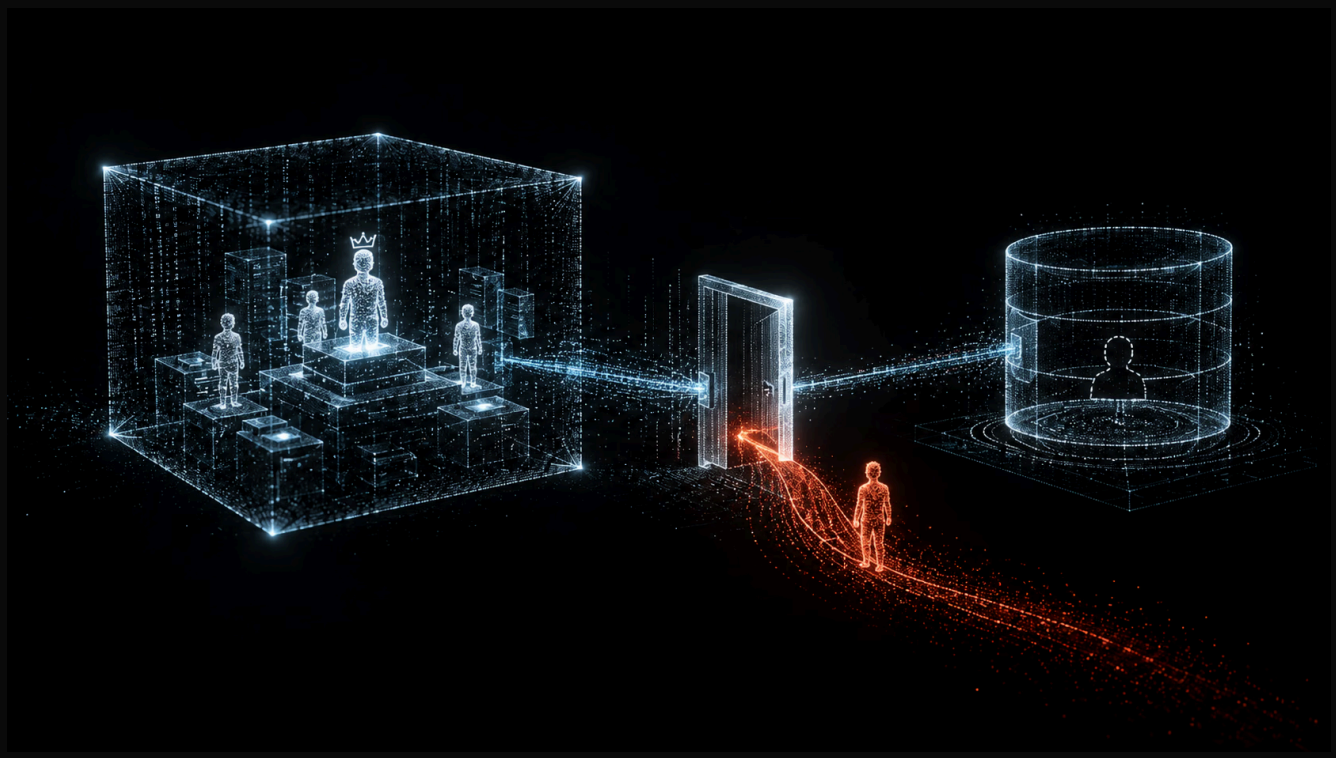
CVE-2026-77226: How an Empty Admin Group Let Anyone Create a Camunda Administrator

CVE-2026-77226 CVSS 9.2



Amartya Jha

Sep 24, 2026



Research

- TL;DR
- At a Glance
- The Reproduction, Up Front
- The Security Boundary: First-Run Setup Must End
- Root Cause: Two Views of Administrator Access
- How the Endpoint Reopens
- Controlled Reproduction
- Which Deployments Could Be Exposed?
- Mitigation and Fix Direction
- Why This Matters
- Credit & Scope

BOOK A DEMO

unauthenticated attacker could create a new administrator account.

TL;DR

- Camunda 7's first-run setup endpoint should refuse requests once an administrator exists. It decides this by counting stored members of the default `camunda-admin` group.
- Camunda's engine can also recognize administrators through configured `adminUsers` and `adminGroups`. The setup check does not inspect those routes.
- If administrators exist through those other routes but `camunda-admin` has no stored members, the setup endpoint can become available again.
- In a local test on Camunda 7 Run 7.24.0, an unauthenticated request created an administrator. The account could deploy a process with a script task; a harmless marker confirmed execution as the Camunda service user.
- This requires a writable identity provider, an empty default admin group, and network access to the Admin webapp. It is not the default state tested, and its prevalence has not been measured.
- Camunda fixed this in 7.24.15, released September 15, 2026. Affected versions are 7.24.0 to 7.24.14. Upgrade to 7.24.15 or later.

At a Glance

Product	Camunda 7 (`camunda-bpm-platform`)
Issue	Critical unauthenticated administrator creation via the first-run setup endpoint
CVE	CVE-2026-77226
Class	Critical Authentication/authorization bypass from divergent definitions of "administrator"
Root cause	The setup gate counts `camunda-admin` membership rows; the engine also honours `adminUsers` and `adminGroups`, which the gate never reads
Impact	One unauthenticated POST creates a full administrator, leading to deployment and script execution (proven to `uid=1000(camunda)`)
Requires	Not the default; four conditions must hold together
Tested on	`camunda/camunda-bpm-platform:run-7.24.0`, source commit `ee4826e5e7`

Severity	9.2, Critical CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
Disclosure	Reported through VulnCheck as CNA. CVE published October 5, 2026: VulnCheck advisory
Found by	**CodeAnt AI Security Research Team**

Camunda needs an unauthenticated way to create the first administrator on a new installation. That access is supposed to end once an administrator exists.

Our research found a state where Camunda already has working administrators, but the setup endpoint cannot see them. The endpoint then treats an existing installation as if it still needs its first administrator.

The Reproduction, Up Front

We tested the difference between a setup gate that correctly closes and one that reopens.

With the default `demo` user still stored in `camunda-admin`, the setup request was refused with HTTP 403 and the message `Setup action not available`. After administrator access was provided through another route and the default group had no stored members, an unauthenticated setup request returned HTTP 204 and created a new administrator.

The new account could deploy a process containing a script task. In our local container, that task wrote the output of `id` to a marker file:

```
uid=1000(camunda) gid=1000(camunda) groups=10
```

The GIF shows the outcome. The rest of this article explains why Camunda reaches two different answers about whether an administrator exists.

The Security Boundary: First-Run Setup Must End

On a new Camunda installation, nobody has administrator credentials yet. The Admin webapp therefore exposes an endpoint to create the initial administrator:

```
POST /camunda/api/admin/setup/{engine}/user/c
```

That behavior is necessary for first-run setup. Its safety depends on refusing the action after an administrator exists.

The relevant check is in `SetupResource.ensureSetupAvailable()`:

```
protected void ensureSetupAvailable(ProcessEr
  if (processEngine.getIdentityService().isRe
      || processEngine.getIdentityService().c
          .memberOfGroup(Groups.CAMUNDA_ADM
```

The check asks two questions:

1. Is the identity provider read-only?
2. Does the identity store have at least one user with a stored membership in `camunda-admin`?

If either answer is yes, setup is refused. A read-only identity provider therefore blocks this path. When a stored member remains in the default admin group, the endpoint also closes as expected.

The problem is that the second question does not cover every way the engine recognizes an administrator.

Root Cause: Two Views of Administrator Access



Camunda's engine can recognize administrators through configured `adminUsers` and `adminGroups`. For group-based access, it considers the groups associated with the current login.

How administrator access exists	Engine recognizes it	Setup check sees it
Stored membership in `camunda-admin`	Yes	Yes
User configured in `adminUsers`	Yes	No
Group configured in `adminGroups`	Yes	Not through that configuration alone

The group case needs care. An administrator group can be present on a person's login without creating a stored membership in the default `camunda-admin` group. The engine can recognize that administrator, while the setup query still counts zero members in the group it examines.

The two functions are not identical. The engine asks whether a particular caller is an administrator; setup asks whether an administrator exists at all. But both decisions rely on a consistent definition of administrator access. Here, that definition has diverged.

How the Endpoint Reopens

The setup check runs for each request. It does not permanently record that first-run setup has finished.

An operator can therefore reach this state after the installation has been running:

1. Administrator access exists through a configured user, another administrator group, or direct authorization.
2. The last stored member of `camunda-admin` is removed.
3. The engine continues to recognize its administrators.
4. The setup endpoint counts zero stored members of `camunda-admin` and permits the setup action, provided the identity provider is writable.

Camunda's administrator authorization plugin can add configured administrator users and groups to the settings the engine reads. The source path examined in this research does not create the default-group membership that the setup check relies on.

Controlled Reproduction

The test used `camunda/camunda-bpm-platform:run-7.24.0` with authentication and authorization enabled.

The negative control came first. While `demo` remained in `camunda-admin`, a setup request returned HTTP 403:

```
{"message":"Setup action not available"}
```

We then kept a working administrator through another authorization route while leaving `camunda-admin` without stored members. The engine recognized the administrator, but the setup check no longer found one through its group query.

An unauthenticated caller obtained a CSRF token available to anonymous requests and sent a request to the setup endpoint. It returned HTTP 204, creating a new administrator.

The account's ability to deploy a process established the next part of the impact. We used a script task only to write a harmless marker inside the local test container. The marker showed execution as `uid=1000(camunda)`.

That result demonstrates the capability gained in the tested environment. It does not establish that every Camunda deployment is exposed or that execution crossed into another system.

Which Deployments Could Be Exposed?

Four conditions must hold together:

Condition	Why it matters

`camunda-admin`	on every request
Reachable Admin webapp	The setup endpoint must be available
Network access to the endpoint	The attacker must be able to send the request

This is **not the default state** in our test. We did not scan deployments or measure how often operators use this configuration. We confirmed the behavior on Camunda 7 Run 7.24.0. Camunda has confirmed the affected versions are 7.24.0 to 7.24.14.

Mitigation and Fix Direction

Fix: upgrade to Camunda 7.24.15 or later. Camunda released the fix on September 15, 2026. Versions 7.24.0 to 7.24.14 are affected. See the VulnCheck advisory.

Operators should also review administrator access after identity-provider changes, group migrations, or removal of the default account.

- **Keep a legitimate stored member in** `camunda-admin` while the setup endpoint is reachable. This maintains the condition on which the setup check relies.
- **Restrict** `/camunda/api/admin/setup/` **after initial provisioning.** New installations still need first-run setup, so provisioning workflows should account for that restriction.
- **Investigate unexpected POST requests to the setup path** after an installation has been configured.

These are operational mitigations. Camunda has fixed this issue in 7.24.15, so upgrading is the recommended remediation. The mitigations above remain useful as defense in depth, or as a stopgap until you can upgrade.

The underlying lesson applies beyond this release: the setup decision must stay consistent with the engine's administrator model. Checking membership in additional stored groups alone would not account for administrator group membership supplied at sign-in by an external identity provider.

Why This Matters

When the default group becomes empty, a legitimate administrator can still use the engine while the gate concludes that no administrator exists. In our local test, that disagreement reopened administrator creation to a caller without credentials.

The general lesson is that a first-run gate must continue to recognize every supported way the system can represent an administrator. Otherwise, changes to access configuration can reopen an action that was meant to be temporary.

Credit & Scope

Finding	CodeAnt AI Security Research Team. The defect, the divergence analysis, the lab reproduction and the code-execution proof are ours.
Not claimed	Deployment-permission-to-script-execution is a long-understood property of BPM engines, not a discovery. It establishes the severity ceiling of the administrator account; no novel exploitation technique is claimed.
Disclosure	CVE-2026-77226, Critical, CVSS 9.2
Testing	Locally-provisioned containers only. Benign markers; nothing destroyed, nothing exfiltrated, no third-party system touched.

> Update: Camunda has fixed CVE-2026-77226 in 7.24.15 (affected: 7.24.0 to 7.24.14). Upgrade to 7.24.15 or later. Advisory: https://www.vulncheck.com/advisories/camunda-incorrect-authorization-via-setupresource-endpoint

References:

- CVE-2026-77226, published October 5, 2026: VulnCheck advisory
- Fixed in Camunda 7.24.15 (released September 15, 2026)

Research conducted against locally-provisioned instances for coordinated disclosure. Line numbers refer to commit `ee4826e5e7` (7.24.0). Every code excerpt is quoted from that tree; every number is from a measured lab run. The CVE record has since been published by VulnCheck; its description may differ in wording from this analysis.

This research is part of an ongoing effort by CodeAnt AI Security Research to audit the trust boundaries in widely deployed infrastructure. Want a deployment or an authorization boundary reviewed? Reach us at securityresearch@codeant.ai

BOOK A DEMO

[FAQ]

Frequently Asked Questions

What is CVE-2026-77226? +

Does this affect every Camunda 7 installation? +

Can this happen after Camunda has already been set up? +

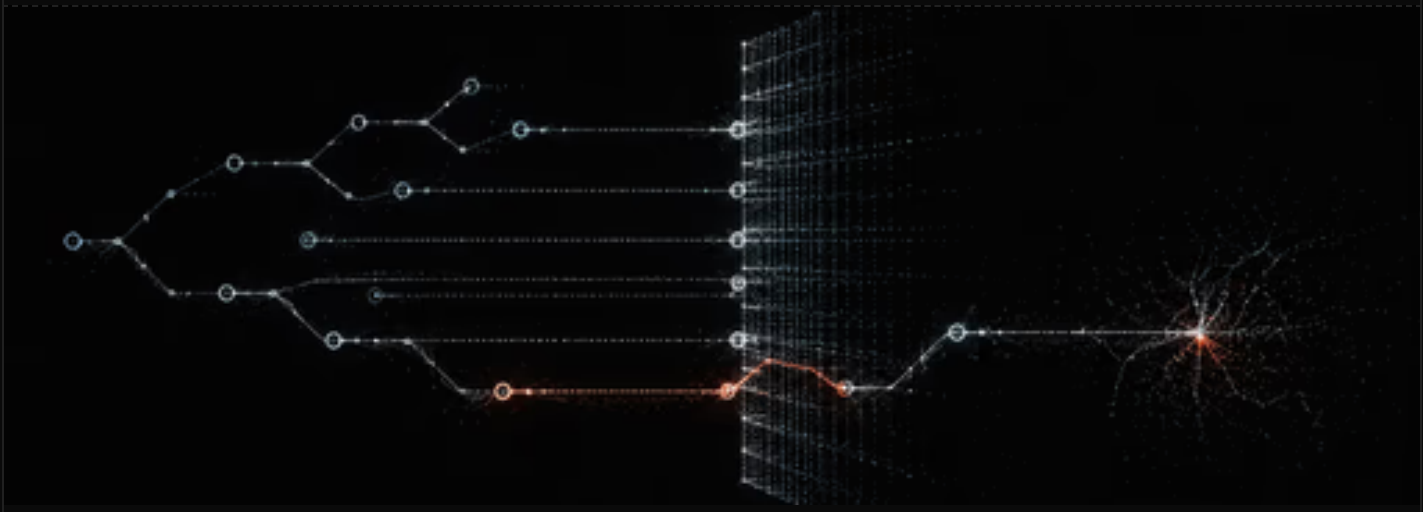
What could an attacker do with the new administrator account? +

How can I check my deployment? +

How do I fix CVE-2026-77226? +

More from CodeAnt

VIEW ALL



Mar 3, 2026

CVE-2026-29000: pac4j-jwt Auth Bypass PoC With a Public Key

CVE-2026-29000 CVSS 10



Mar 9, 2026

CVE-2026-28292: simple-git RCE via Case-Sensitivity Bypass

CVE-2026-28292 CVSS 9.8



Mar 11, 2026

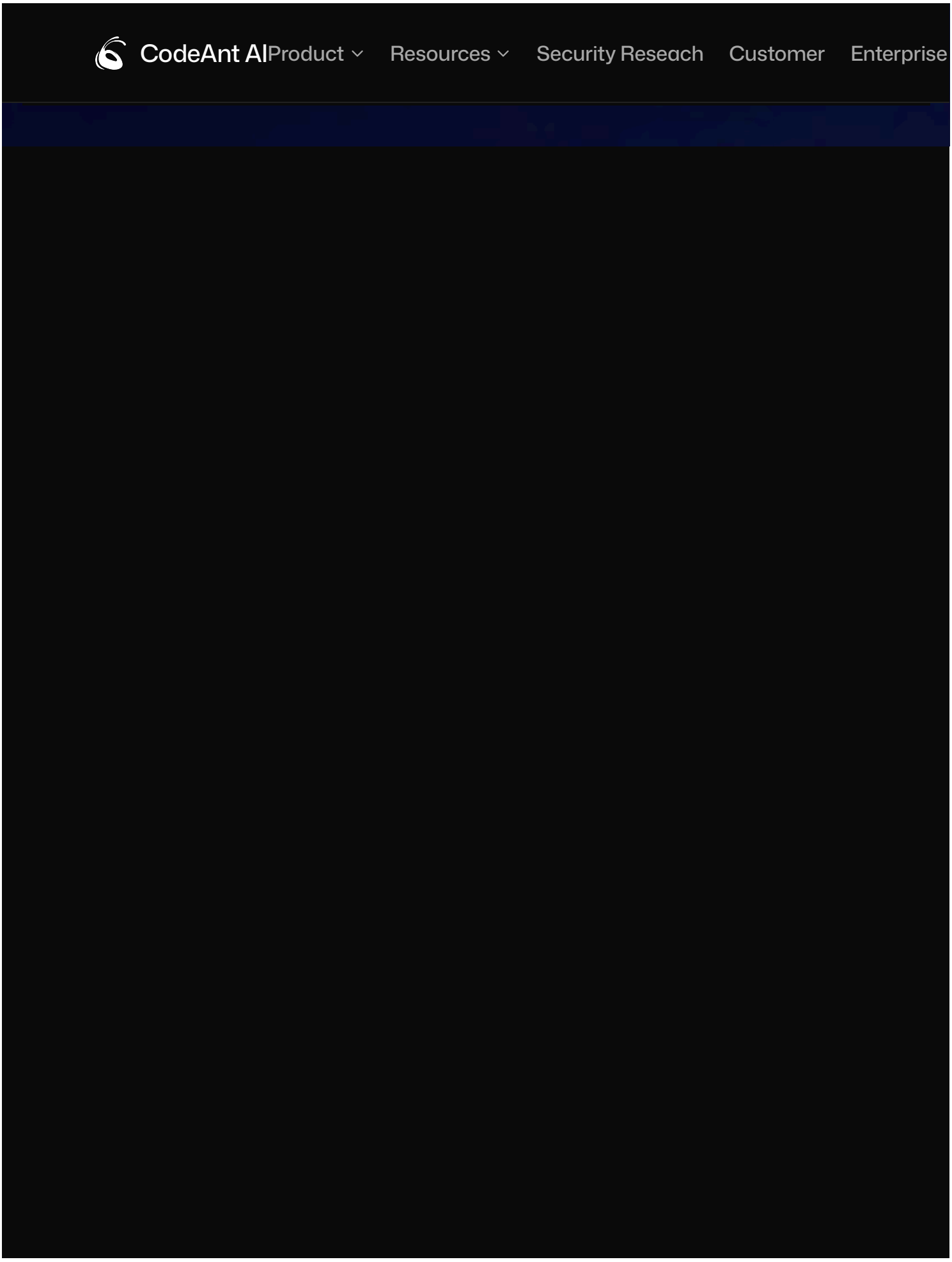
CVE-2026-31988: jszip DoS via Malformed ZIP File

CVE-2026-31988 CVSS 6.9

[GET STARTED]

Find out what's already exploitable in your codebase.

START PENTEST BOOK A DEMO


CodeAnt AI
Product
Resources
Security Reseach
Customer
Enterprise