

nextlevelbuilder / goclaw Public[Code](#) [Issues 126](#) [Pull requests 116](#) [Discussions](#) [Actions](#) [Projects](#)[New issue](#)

critical: unauthenticated log subscription and command injection in heartbeat execution flow #866

Closed#950

Labels

P0-criticalarea:securitybug

CH13hh opened 3 weeks ago · edited by CH13hh

Edits ▾ ⋮

Title: Critical Authentication Bypass and Default Permit Policy Leading to Unauthenticated Remote Command Execution via Heartbeat Injection

Severity: Critical (CVSS 3.1 Score: 10.0 - AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

Affected Components:

gateway/connect (Authentication Interceptor / Middleware)

authorization/rbac (Permission Policy Engine)

api/channels/instances (Instance Listing RPC)

api/logs (Log Streaming RPC)

heartbeat/runner (Heartbeat Execution Engine)

Vulnerability Type:

CWE-306: Missing Authentication for Critical Function

CWE-863: Incorrect Authorization

CWE-94: Improper Control of Generation of Code ('Code Injection')

Description

GoClaw's Connect gateway exhibits a critical flaw in its authentication enforcement logic. When a client connects with an invalid, expired, or missing Bearer token, the server does not reject the connection. Instead, it silently downgrades the connection to an authenticated context with the viewer role.

Concurrently, the RBAC permission engine operates under a default-permit policy for unclassified RPC methods. Any method not explicitly restricted is inadvertently exposed to the viewer role.

By exploiting this chain of weaknesses, an unauthenticated remote attacker can:

Establish a "degraded" viewer session without any valid credentials.

List all registered agents and obtain their raw agent_id (UUID).

Subscribe to arbitrary agent logs via logs.tail to confirm liveness.

Write malicious content to the agent's heartbeat.set or heartbeat.checklist.set endpoints.

Trigger the Heartbeat Runner, which injects the attacker-controlled prompt/checklist content into the agent's execution context (specifically into a HEARTBEAT.md or immediate prompt payload).

Leverage the agent's exec tool capability (if enabled) to achieve arbitrary command execution on the underlying host via sh -c.

Remediation Recommendations

Reject Unauthenticated Connections (Critical):

Modify the Connect interceptor to strictly close the connection or return Unauthenticated status for any token verification failure. Do not fall back to a default viewer context.

Enforce Default Deny (Critical):

Change the RBAC engine policy to Default Deny. RPC methods must be explicitly annotated with allow: [viewer] or allow_unauthenticated: true if public access is intended.

Scoped Authorization for Heartbeat:

Heartbeat write operations (heartbeat.set) must never be accessible to the viewer role. These should require agent:write or admin scope.

Input Sanitization in Runner:

Treat any content originating from the heartbeat service as tainted/untrusted data. The Heartbeat Runner should sandbox or strictly validate the prompt before concatenating it with the agent's instruction stream. Consider using a dedicated, read-only context for heartbeat checks that does not permit access to exec tools.

Mask Sensitive Identifiers:

The channels.instances.list endpoint should return a non-sensitive Alias or Fingerprint instead of the raw internal UUID unless the caller possesses admin scope.

```
[+] heartbeat prompt/checklist written by viewer
[+] heartbeat.test triggered
[+] execution proof
{
  "mode": "run.completed",
  "frame": {
    "type": "event",
    "event": "agent",
    "payload": {
      "type": "run.completed",
      "agentId": "textel-man-...",
      "runId": "i-...",
      "payload": {
        "content": "app\\nbin\\ndev\\netc\\nhome\\nlib\\nmedia\\nmnt\\nopt\\nproc\\nroot\\nrun\\nsbin\\nsrv\\nsys\\ntmp\\nusr\\nvar",
        "usage": {
          "cache_creation_tokens": 0,
          "cache_read_tokens": 0,
          "completion_tokens": 92,
          "prompt_tokens": 1523,
          "total_tokens": 1615
        }
      }
    },
    "channel": "heartbeat",
    "sessionKey": "a-..."
  }
}
[+] cleanup applied: prompt/checklist cleared, enabled=false
```

Email: aibsec@tiansu.org

thieung added bug P0-critical area:security [2 weeks ago](#)

thieung added a commit that references this issue [2 weeks ago](#)

fix(security): close auth bypass + default-permit RBAC (issue [nextlev.](#) ...)

2319c5c

thieung mentioned this [2 weeks ago](#)

[fix\(security\): close auth bypass + default-permit RBAC \(issue #866\) #950](#)

thieung added 2 commits that reference this issue [2 weeks ago](#)

chore: move [nextlevelbuilder#866](#) repro scripts into PR description ...

72ba2ec

fix(security): close auth bypass + default-permit RBAC (issue [nextlev.](#) ...)

42f598b

viettranx added a commit that references this issue [2 weeks ago](#)

fix(security): close auth bypass + default-permit RBAC (issue [#866](#)) (: ...)

406022e

viettranx closed this as [completed](#) in [#950](#) [2 weeks ago](#)

viettranx mentioned this [2 weeks ago](#)

[fix\(acp\): Gemini ACP protocol fixes and multi-session architecture #901](#)

duhd-vnpay added a commit that references this issue [2 weeks ago](#)

chore(goclaw): merge upstream v3.9.0 – tenant-scoped web_search + sec. ...

2c19549

vanducng added a commit that references this issue [5 days ago](#)

fix(permissions): classify zalo.webhook_url RPC as admin ...

fe301f6

[Sign up for free](#) to join this conversation on [GitHub](#). Already have an account? [Sign in to comment](#)

Metadata

Assignees

No one assigned

Labels

P0-critical **area:security** **bug**

Type

No type

Projects

No projects



Milestone

No milestone

Relationships

None yet

Development

 [fix\(security\): close auth bypass + default-permit RBAC \(issue #866\)](#)
nextlevelbuilder/goclaw
 **v3.9.0**

Participants

