ISSUE #003 · SANDBOX & CONTROL-PLANE ISOLATION

AuthZ said deny. The parser said yes.

A one-megabyte padding trick that walks around Docker's last line of defense, the AWS session-policy pattern for forensic artifact collection, and the Kubernetes 1.36 features that quietly change who can impersonate whom.

> ATTACK

Cyera Research · Vladimir Tokarev · 2026-04-07 · **One Megabyte to Root: How a Size Check Broke Docker's Last Line of Defense**

Docker's authorization middleware hands a request body to your AuthZ plugin. Except when the body is over one megabyte. Then the middleware silently hands the plugin `RequestBody: nil`, the plugin has nothing to reject, and the daemon processes the full request anyway.

```
# the bypass in one request POST /containers/create {"Privileged": true, "Binds": ["/:/host"], "_padding": "<1MB+ of bytes>"}
```

Container starts, host root mounts inside, you read `/root/.ssh/id_rsa`, `/etc/kubernetes/admin.conf`, whatever your agent needs. CVE-2026-34040 (CVSS 8.8 GHSA / 7.8 NVD). Engine 1.10 (Feb 2016) introduced AuthZ middleware. CVE-2024-41110 patched the `Content-Length: 0` bypass in July 2024. This new CVE uses the oversize path nobody had tested. Cyera notes the same failure mode is already seen in AI coding agents bypassing sandbox layers autonomously to complete tasks.

▸ MONDAY CHECK

If any host runs Docker Engine <29.3.1 and the AuthZ plugin is part of your sandbox (Twistlock, OPA-docker-authz, custom webhook), patch this week. Can't patch: nginx in front of the socket with `client_max_body_size 512k;`, socket locked to local users. Deeper question: if the AuthZ plugin is the only thing between your agent and host root, that's a single silent failure away from a bad afternoon.

> RULE

Detection sketch for the AuthZ-bypass pattern. If your Docker daemon proxies through nginx or envoy, alert on any POST to `/containers/create` or `/containers/*/exec` where Content-Length > 1MB. That's the fingerprint; padded JSON doesn't fit legitimate workflows. If you don't proxy the socket, enable `"debug": true` in `/etc/docker/daemon.json` and grep `/var/log/docker.log` for `Request body is larger than`, the warning Docker logs when it drops the body. Under 20 minutes as an nginx rule or Splunk query.

> DEFENDER

AWS Security Blog · Jason Garman + Vaishnav Murthy · 2026-04-08 · **A framework for securely collecting forensic artifacts into S3 buckets**

Deploy the forensic-artifact S3 framework before you need it. Session-policy-scoped IAM grants upload to a single case prefix (`arn:aws:s3:::forensics-collection/CASE-NNNN/*`), KMS at rest, Object Lock for immutability, CloudTrail data events. No long-lived keys on responding hosts. Three CDK stacks at `aws-samples/sample-collect-forensic-artifacts-s3`.

Synacktiv · Noam Leipold · 2026-03-26 · **Kubernetes forensics 1/3: what the container?**

Part one walks `/var/lib/docker/overlay2/`, `containers/<id>/config.v2.json`, and the tools (`dive`, `diffoci`, `docker-explorer`) for runtime changes. Pre-draft the first three commands you'd run on a compromised host.

> RADAR

Sysdig · Victor Jimenez Cerrada · 2026-04-15 · **Kubernetes 1.36 - New security features**

Three changes to attack-path assumptions. Fine-grained Kubelet API authorization (stable): `nodes/proxy` no longer grants everything, `nodes/pods` alone is grantable. Constrained impersonation (beta): limits what one account can do when impersonating another. User namespaces (stable): container escapes land unprivileged, not root.

SOURCES

Cyera / cyera.com/research/one-megabyte-to-root-how-a-size-check-broke-dockers-last-line-of-defense
AWS / aws.amazon.com/blogs/security/a-framework-for-securely-collecting-forensic-artifacts-into-s3-buckets
Synacktiv / synacktiv.com/publications/kubernetes-forensics-13-what-the-container
Sysdig / sysdig.com/blog/kubernetes-1-36-new-security-features