2022-02-24 Registry Advisory

Summary

Registry v3.3.0 introduced CO-specific API users, which can be either privileged (having full access to the CO via the API) or unprivileged (having no specific access unless granted). An undocumented behavior of the underlying framework created the possibility of data leakage for certain API requests.

Severity

The severity of this issue is *medium*, as a privileged API user is required to leak data.

Exposure

The exposure will generally be *low*, as this advisory only meaningfully affects multi-tenant deployments, and only those that have enabled CO-specific API users.

Recommended Mitigation

Deployments not using the described configuration need not take any action, though should plan an upgrade as soon as plausible in case CO-specific API users are created later.

Deployments using the described configuration should immediately upgrade to Registry v4.0.2, or to develop commit 0712c7a918 or later.

Deployments may also perform an audit, as described in *Discussion*, below.

Alternate Mitigations

Deployments may alternately disable any privileged CO-specific API users until an upgrade can be performed.

Discussion

Registry v3.3.0 introduced CO-specific API users, which can be either privileged (having full access to the CO via the API) or unprivileged (having no specific access unless granted). Previously, the REST API was only available to platform-wide superusers.

An undocumented behavior of the underlying framework allows for a specifically crafted REST request to be misinterpreted and return data the CO-specific API user is not authorized to view. This behavior does *not* allow for the unauthorized editing of records, only viewing them.

Auditing access may be possible by reviewing web server logs for REST API requests that are not conformant to the documentation or, if sufficient logging is enabled, return documents significantly larger than might otherwise be expected.

Acknowledgments

The COmanage Project wishes to thank CILogon for reporting this issue, and Scott Koranda and Ioannis Igoumenos for their extensive work in addressing this issue and performing a comprehensive review of the REST API for this release.

References

- CO-2146
- CO-2294
- CO-2341