2017-01-30 Registry Advisory

- Summary
- Severity
- Exposure
- Recommended Mitigation
- Alternate Mitigations
- Discussion
- References

Summary

As part of a routine code review, a potential vulnerability was discovered affecting Registry versions 0.9.1 through 1.0.5.

Severity

The severity of this vulnerability will vary according to a given configuration, but will likely be High or Very High for most deployments.

A configuration with administrator-only enrollment flows and no user self service is not affected by this issue.

Exposure

The exposure from this vulnerability is expected to be very low, as it is unlikely that this vulnerability has been exploited.

Recommended Mitigation

Upgrade to COmanage Registry v1.0.6 or later.

Deployments using the *develop* branch may pull the latest code from that branch.

Alternate Mitigations

The project will be unable to provide any support or patches for earlier versions. Due to the way the fix was implemented, it is non-trivial to backport.

Discussion

Various forms did not properly sanitize user input, resulting in situations where the unsanitized data could be rendered in a view. For example, a malicious user could have included JavaScript in their name such that when an administrator viewed their record the JavaScript executed. As part of addressing this issue, both input validation and output filtering routines were improved throughout the application.

Since Registry operates using copy-on-write (available since v0.9.2 or v0.9.4 depending on the table), user data is not deleted from the database, even when changed. It is possible to audit tables containing user-managed data to see if any exploits were attempted. For self service enrollment flow, check cm_co_petition_attributes. For self service attributes, check the appropriate tables associated with enabled self service (eg: cm_names).

References

- CO-1369