2018-05-30 Registry Advisory

Summary

The default layout view used by COmanage Registry beginning with version 0.9.4 and continuing through version 3.1.0 did not properly sanitize certain variables that contained user input. As such, these versions are susceptible to HTML injection attacks.

Severity

Very High. The bug is remotely exploitable without authentication, though only by tricking a user into opening an appropriately crafted URL.

Exposure

Unknown, but probably Low. We are unaware of any reports of exploits related to this bug, and the bug itself does not directly compromise user data.

Note that the Chrome browser appears to detect and block at least some attempts to exploit this issue.

Recommended Mitigation

Upgrade to COmanage Registry v3.1.1 or later.

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

Alternate Mitigations

It is possible to manually backport the patch to earlier versions. The diff against v3.1.1 is available here, though the changes may need to be manually applied to older versions.

Discussion

CakePHP is an MVC (Model-View-Controller) framework that uses PHP variables to communicate data between the controllers and views. Some of these variables contain unfiltered, user controllable data.

A change introduced in v0.9.4 incorrectly used unfiltered variables to construct a class name for the main body tag used in the default layout for most views, including the unauthenticated view presented before a user logs in. A carefully constructed URL can render this view with user-defined HTML injected into the body tag, with specific results dependent on the browser involved.

Acknowledgments

Thanks to Bas Zoetekouw and Niels van Dijk at SURFnet who reported the issue to the Project based on a report to them by a third party.

References

- CO-1621