COmanage Registry Security Advisories

- Security Advisories
    - Severities
- Security Advisory Policy
- See Also

If you would like to report an issue you believe is security related, please open a new JIRA Issue. Be sure to set the following attributes:

- Project: **COmanage (CO)**
- Issue Type: **Bug**
- Security Level: **Vulnerability**
- Component: **Registry**

Alternately, you may notify comanage@sphericalcowgroup.com. Do *not* email the users or developers lists, as those are public.

In general, you should always upgrade to the latest version of COmanage as soon as practical, upgrading a QA or test server first. The further behind you fall, the harder it will probably be to upgrade if a highly critical security advisory is released.

Security Advisories

Advisory	Affected Releases	Severity	Exposure
2015-12-09	0.9.4 and earlier	Unknown	Unknown
2017-01-30	0.9.1 through 1.0.5	High or Very High	Low
2018-05-30	0.9.4 through 3.1.0	Very High	Low or Medium
2020-05-29	3.2.4 and earlier	Unknown	Low
2020-10-29 *	3.2.0 through 3.3.0	Medium	Low
2021-05-24a	3.3.0 through 3.3.2	Medium	Low
2021-05-24b *	0.5 through 3.3.2	Very High	Varies
2021-12-07	3.3.0 through 4.0.0	Medium	Low
2022-02-24	3.3.0 through 4.0.1	Medium	Low

** Advisories that describe unexpected behavior from a supported configuration, not a code exploit*

Severities

- Very High: Remotely exploitable without authentication
- High: Exploit requires authentication as any user
- Medium: Exploit requires authentication as any administrator
- Low: Exploit requires authentication as a platform administrator, or requires command line login access to server

Security Advisory Policy

1. In general, please report security advisories to the email address at the top of this page. While we can create closed JIRA issues that are not publicly visible, you as the reporter may not be able to do so, and we'd rather not share information to the public until we are ready.
2. Once the problem has been identified and a fix prepared, we will schedule a release date and make a public announcement. We will typically attempt to make the announcement 1 to 2 weeks ahead of the release date, however conditions may require a shorter or longer Announcement Period.
3. After the public announcement but before the release date, no details about the issue will be made public.
4. During the Announcement Period, we reserve the right to provide early access to selected deployers in order to ensure proper quality control and testing. Our expectation is that anyone who receives early access to the fix will not share it further without our permission.
5. On the release date, we will simultaneously release both the fix (typically as a new maintenance release) as well as the technical details. Deployers should be prepared to apply the fix as soon as possible on the release date. (As on open source project, the fix will be public, and so there is limited -- if any – value in delaying release of the technical details.)
6. Currently, the COmanage developers are unable to commit to providing security fixes for any version other than the latest release. Depending on the details of any given fix, it may or may not be plausible to backport fixes to earlier releases.

See Also

- COmanage Match Security Advisories