CBAS Web Advisory--2019-5-9

Overview

Several security vulnerabilities in CBAS Web were recently found by security company Applied Risk. The vulnerabilities discovered as follows:

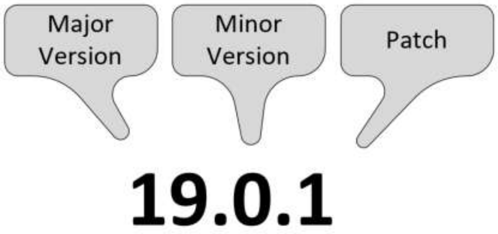
- Unauthenticated Cross-Site Scripting (XSS) vulnerability on login page and forgot-password page, including User-Agent when debugging is enabled in verbose mode.
- Authenticated Blind SQL Injection affecting multiple GET/POST parameters.
- User enumeration weakness.
- Authentication bypass.
- Command execution via python calling os.system().
- Firmware source code disclosure via unprotected Subversion directory.
- Cross-Site Request Forgery (CSRF) on all submission forms.
- Hard-coded encryption key for database backup decryption of full MySQL dump.
- Insecure storage of passwords using MD5 algorithm (prefix ‘pw’).
- Default credentials

Mitigation

Each of these vulnerabilities were addressed, patched and verified for all currently supported major versions of CBAS Web. These patches were then officially released along with updated version numbers. We also contacted all clients with software maintenance agreements as well as those to whom we regularly provide support, and updated their sites to the latest version.

How to Determine if You’ve Been Patched

Computrols software products employ the common and well-defined version control methodology known as Semantic Versioning. The main (3) numbers that you see in our software product versions are defined as follows:



To find out if your CBAS Web software is one that contains the necessary patches for these vulnerabilities, locate the version number at the top right corner of the CBAS Web Heading on your site. Use the Major Version number to reference the required Minor and Patch numbers listed below:

Major Version 19	19.0.1 (or greater)
Major Version 18	18.0.1 (or greater)
Major Version 15	15.0.1 (or greater)
Major Version 14	14.0.1 (or greater)
Major Version 8	8.0.7 (or greater)
Major Version 7	7.2.1-*Beta* (or greater)
Major Version 8	6.9.2 (or greater)
Major Version 4	4.8.2 (or greater)
Major Version 3	3.15.1 (or greater)

What to do if you Need a Patch

If your current CBAS Web version is old and needs to be updated, please contact Computrols Technical Support. One of our technical representatives will be happy to provide you with a patched version and assist you in updating your site.