CBAS Web 19.x.x Changelog

Product: CBAS Web, Major Version: 19.x.x

2020-01-17: Security patches

- Apache 2.4.x Multiple Vulnerabilities
  - A privilege escalation vulnerability exists in module scripts due to an ability to execute arbitrary code as the parent process by manipulating the scoreboard. (CVE-2019-0211)
  - An access control bypass vulnerability exists in mod_auth_digest due to a race condition when running in a threaded server. An attacker with valid credentials could authenticate using another username. (CVE-2019-0217)
  - An access control bypass vulnerability exists in mod_ssl when using per-location client certificate verification with TLSv1.3. (CVE-2019-0215)
  - In addition, Apache httpd is also affected by several additional vulnerabilities including a denial of service, read-after-free and URL path normalization inconsistencies.

  Upgrade Apache2 server to ver. 2.4.41, where the above vulnerabilities have been fixed.

- Disability of phpmyadmin - SQL injection (SQLi) vulnerability exists in phpMyAdmin due to improper validation of user-supplied input

2019-01-12: Updates to Version 19.0.1

- Added more options for the mass import of access control cards through means of cvs spreadsheet.
- New interface for uploading mass collection of pictures for access cards.
- Added feature to select access control group on mass import.
- New operation tools for multiple selection of access cards.
- Distributed new access control badge templates
- Support for Ubuntu 16 and above provided.

2019-04-10: Released Version 19.0.1

- Vulnerability found by Security Company Applied Risk. Patched in this release.
- Removed aggregate authentication mode
- Strong passwords enforcement

- Improved security on the following:
- Cookies
- Cross-origin Resource Sharing
- HTTP Public Key Pinning
- HTTP Strict Transport Security
- Redirection
- Referrer Policy
- Subresource Integrity
- X-Content-Type-Options
- X-Frame-Options
- X-XSS-Protection
- Defended against html injection on the *Login* and *Reset Password* pages
- Removed user enumeration issue on failed logins.

2019-03-20: Released Version 19.0.0