AR2019009

Computrols CBAS-Web 18.0.0 Multiple Vulnerabilities

Author: Gjoko Krstic

Release Date: May 10, 2019

Copyright Notices

COPYRIGHT NOTICE

OVERVIEW

Multiple vulnerabilities were found in the Computrols CBAS-Web Building Management System (BMS). These findings include Cross-Site Scripting, Cross-Site Request Forgery, Username Enumeration, Source Code Disclosure, Default Credentials, Hard-coded Encryption Key, Authenticated Blind SQL Injection, Authentication Bypass, Authenticated Command Injection and Mishandling of Password Hashes.

AFFECTED PRODUCTS

Computrols CBAS;

The following versions are affected:

- 18.0.0 and below

The vulnerabilities have been discovered and validated in Computrols CBAS-Web 18.0.0. Older versions are affected too.

IMPACT

An unauthenticated user can gain full system access.

BACKGROUND

Computrols was founded in 1983 and first began as a service business, providing maintenance for the large building automation systems of the day. Computrols Building Automation Software (CBAS) is the simplest building automation system software to install, program, maintain, and operate.

VULNERABILITY DETAILS

Default Credentials

Attackers can easily obtain default passwords and identify Internet-connected target systems. Passwords can be found in product documentation and compiled lists available on the Internet. It is possible to identify exposed systems using search engines like Shodan, and it is feasible to scan the entire IPv4 internet.

Applied Risk has calculated a CVSSv3 score of 9.8 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.

Cross-Site Request Forgery

The affected application allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site.

Applied Risk has calculated a CVSSv3 score of 5.0 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L.

Username Enumeration

The application suffers from a username enumeration weakness. The device behaves differently or sends different responses in a way that exposes security-relevant information about the state of the product, such as whether a particular operation was successful or not.

Applied Risk has calculated a CVSSv3 score of 5.3 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N.

Cross-Site Scripting

The application suffers from a reflected XSS vulnerability. The issue occurs when input passed via several parameters to several scripts is not sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

Applied Risk has calculated a CVSSv3 score of 5.4 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N.

Command Injection

The application constructs an OS command using externally-influenced input from an upstream component, but incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component. This could allow authenticated attackers to execute unexpected, dangerous commands directly on the operating system.

Applied Risk has calculated a CVSSv3 score of 8.8 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H.

Source Code Disclosure

The application has an unprotected Subversion directory that anyone can access. This allows an attacker to download the entire firmware codebase and disclose sensitive information about the innerworkings of the underlying OS. Directory indexing was also enabled for several directories disclosing various scripts and sensitive information.

Applied Risk has calculated a CVSSv3 score of 7.5 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N.

Hard-coded Encryption Key

The application suffers from a hard-coded encryption key for database backup file decryption. The issue resides in several scripts obtained with direct access or by downloading the exposed Subversion directory. This can aid an authenticated attacker to gain access to the full database of the device and disclose sensitive information.

Applied Risk has calculated a CVSSv3 score of 6.5 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N.

Authenticated Blind SQL Injection

The vulnerability exists due to insufficient filtration of multiple HTTP GET and POST parameters passed to different scripts. A remote authenticated attacker can execute arbitrary SQL commands in the application's database.

Applied Risk has calculated a CVSSv3 score of 6.3 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L.

Authentication Bypass

The application suffers from an authentication bypass vulnerability. Calling agg_post action in auth.php script will trigger the AggregatePost function. This function expects a code-parameter and it will check it against a list of views. If the view code matches, the cookie's session will get the username 'aggregate' set and the application will enable the auth flag. This allows an unauthenticated attacker to bypass authentication and have full control of the device.

Applied Risk has calculated a CVSSv3 score of 8.1 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H.

Mishandling of Password Hashes

The application stores the passwords in the database using the MD5 hash. The MD5 algorithm is vulnerable to known cryptographic attacks.

Applied Risk has calculated a CVSSv3 score of 5.3 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N.

MITIGATION

Computrols is aware of the reported vulnerabilities and has addressed the issues with a new firmware version.

REFERENCES

Vendor website

http://www.computrols.com/

Product page

http://www.computrols.com/building-automation-software/

Common Vulnerability Exposure (CVE):

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10846
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10847
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10848
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10849
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10850
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10851
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10852
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10853
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10854
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10855

Vendor Advisories:
http://www.computrols.com/support/documentation/
http://www.computrols.com/wp-content/uploads/2019/05/CBAS-Web-Advisory-2019-5-9.pdf

CONTACT DETAILS

For any questions related to this report, please contact Applied Risk Research team at:

Email: research@applied-risk.com

PGP Public Key:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQENBFOgiBQBCACj+Notofe/liuHuc90yy8GAfFn8YFCsMCo7wQmQRNTT43bZQq2
gQr7FTLtOl6rBkOLm8bDk0YY/CtWsjdLh1jlDrWyfU6yIzfcu4CSpn1+5n1ivNN5
17ri+VtmgF392twiKhy2+MC9O4of+GMyu1hy5pIjwi3qGzdNlAnT7m7U/hNzaIR4
ae7+NuWtEvWWKyp3IEEMKTDV/ZOtRD1tfIR8KeBB7Axa8cJdlotw/Ail9TLVB6kt
a/BlvhM/zgWfbEPadnx6B0u7pdW50bTECAs0VHje8mcheTwTCAJo+de3/DqUA34X
oF9aAZWpZWE7VH0O4Q8ZtfrXPFqR2xF8LHhZABEBAAG0REFwcGxpZWQgUmlzayBS
ZXNlYXJjaCBUZWFtIChubyBwYXNzd29yZCkgPHJlc2VhcmNoQGFwcGxpZWQtcmlz
ay5jb20+iQE+BBMBAgAoBQJToIgUAhsjBQkJZgGABgsJCAcDAgYVCAIJCgsEFgID
AQIeAQIXgAAKCRA6nyA79MpeSay8CACSI4UhAget5Z+qEDmz1fe+9krgmx7wwDnF
ig4AVICU8ppJQoUCB5pP6eIV/DM7i+mu8e9zeGlA82t69yTVIANWx72zPmGn5Ku8
4t79gR8V+99PW+O+1rej+96wfL2v+IuOXOcJkTsheUyQZ8Klwc1U8kTdGZEY+/IZ
c32ZhyJ04/cchVP/Zsj2WQIh84wbqa27bTEyyFBnD8FdQ2R4UDTqwACbLgp82m29
P346s80c15RZIX8wUAu0LcNbWJJHRsX6Sa+MozTNug9yWdpZt+nmHEMl95lJYktR
w3+gwyaXeUxALX8Baq2EJDdNx9OlsryiNFdnE9vKIM0+24fTDoqguQENBFOgiBQB
CACtSAm5oBD4kJJY+rtHh6xoytOzP6bFEnrVjqXrXCj+ECG6+N6Droqd072X5hki
qoL1viI4NV+2jrYTtMIu+/nc4zuUFUDRYSm0X/K3WgsqaLA4jdedTm45Tau/Fn6W
26tB5AaddcoDdx6JVGIxFvwU+41KoZ7ouDZo7UEBZ7getPubyR4aPepUsjYnPOUL
0SHH76+b/pC5AZm4crpqWf7Q+qaYQdBIhJbgm5ijFzCyHusYgVGBT1hak81QGpM0
1K9wXki/fJrRyEsWWUjpVSEPRizsFJ60v+NrX50gvvXed8MlX0O9efwgeCmGIVDL
oxF/AmnznYWy0LYWAhh/dW7dABEBAAGJASUEGAECAA8FAlOgiBQCGwwFCQlmAYAA
CgkQOp8gO/TKXkmgdQf/ZtwhL2bs+mlmTUmlT3XO4ekVPRLQKtBYfr8y4rdfnq7Y
MdFYEJAt45R+e4I3I7cIJM1/ImncjFng1EpwFItAXVLa1ktiO6BqT6wBqL6pSBe3
2x5VP8OEnnRubCgYaTotNfiEErgh8cG92tW/TiQArU2dnBcVwYHVwPm450pEv9Aq
BBzgeZ25I1Cv0vlQkQLy9PuTA6DWoxeIxbaMD8ZpKGi+XDrfguJ3tERQMlUA6Fc+
OBkT/NKz8mgecVrwCWbCmScyEhh6onTkevI+mydvsxYG8rE6YVxl3oK5Xi6tvAt9
cUPKKK363nkA1AEoMvTz1bCbmTGvTNWLifoMNtNnGA==
=pAvd
-----END PGP PUBLIC KEY BLOCK-----
```