Proactive Notification: Advisory

March 29, 2018

CA Workload Automation AE and CA Workload Control Center customers, please review the following security notice.

For the latest version of this security notice, see

CA20180329-01: Security Notice for CA Workload Automation AE and CA Workload Control Center

CA20180329-01: Security Notice for CA Workload Automation AE and CA Workload Control Center

Issued: March 29, 2018
Last Updated: March 29, 2018

CA Technologies Support is alerting customers to two potential risks with CA Workload Automation AE and CA Workload Control Center. Two vulnerabilities exist that can allow a remote attacker to conduct SQL injection attacks or execute code remotely.

The first vulnerability, CVE-2018-8953, in CA Workload Automation AE, has a medium risk rating and concerns insufficient data validation that can allow an authenticated remote attacker to conduct SQL injection attacks.

The second vulnerability, CVE-2018-8954, in CA Workload Control Center, has a high risk rating and concerns an Apache MyFaces configuration that can allow an authenticated remote attacker to conduct remote code execution attacks.

Risk Rating

CVE-2018-8953 – Medium
CVE-2018-8954 - High

Platform(s)

All supported platforms

Affected Products

CVE-2018-8953:
CA Workload Automation AE r11.3.5, r11.3.6 SP6 and earlier
CVE-2018-8954:
CA Workload Control Center (CA WCC) r11.4 SP5 and earlier

Unaffected Products

CA Workload Automation AE r11.3.5 with appropriate fixes listed below
CA Workload Automation AE r11.3.6 SP7
CA Workload Control Center (CA WCC) r11.4 SP5 with appropriate fixes listed below
CA Workload Control Center (CA WCC) r11.4 SP6

How to determine if the installation is affected

Customers may use the CA Workload Automation AE / CA Workload Control Center interface to find the installed version and then use the table in the Affected Products section to determine if the installation is vulnerable.

Solution

CA Technologies published the following solutions to address the vulnerabilities.

CA Workload Automation AE r11.3.5:
Apply the appropriate patch for your platform:
Windows: SO00700
HP: SO00696
AIX: SO00695
Sun: SO00694
Linux: SO00693
CA Workload Automation AE (AutoSys Edition) r11.3.5 Solutions & Patches

CA Workload Automation AE r11.3.6:
Apply SP7.
CA Workload Automation AE Release 11.3.6 SP7 General Availability Announcement

CA Workload Control Center (CA WCC) r11.4 SP5:
Apply patch RO99200
CA Workload Control Center Solutions & Patches

CA Workload Control Center (CA WCC) r11.4 SP6:
CA Workload Automation AE Release 11.3.6 SP7 General Availability Announcement

References

CVE-2018-8953 - CA Workload Automation AE SQL injection
CVE-2018-8954 - CA Workload Control Center MyFaces RCE

Acknowledgement

CVE-2018-8953 – Hamed Merati from Sense of Security Labs
CVE-2018-8954 – Hamed Merati and Kacper Nowak from Sense of Security Labs

Change History

Version 1.0: 2018-03-29 - Initial Release

CA will send a notification about this security notice to customers who are subscribed to Proactive Notifications.

If additional information is required, please contact CA Technologies Support at http://support.ca.com/.

If you discover a vulnerability in a CA Technologies product, please send a report to the CA Technologies Product Vulnerability Response Team.

CA Technologies security notices