CA Workload Automation AE / CA Workload Control Center SQL Injection / Code Execution

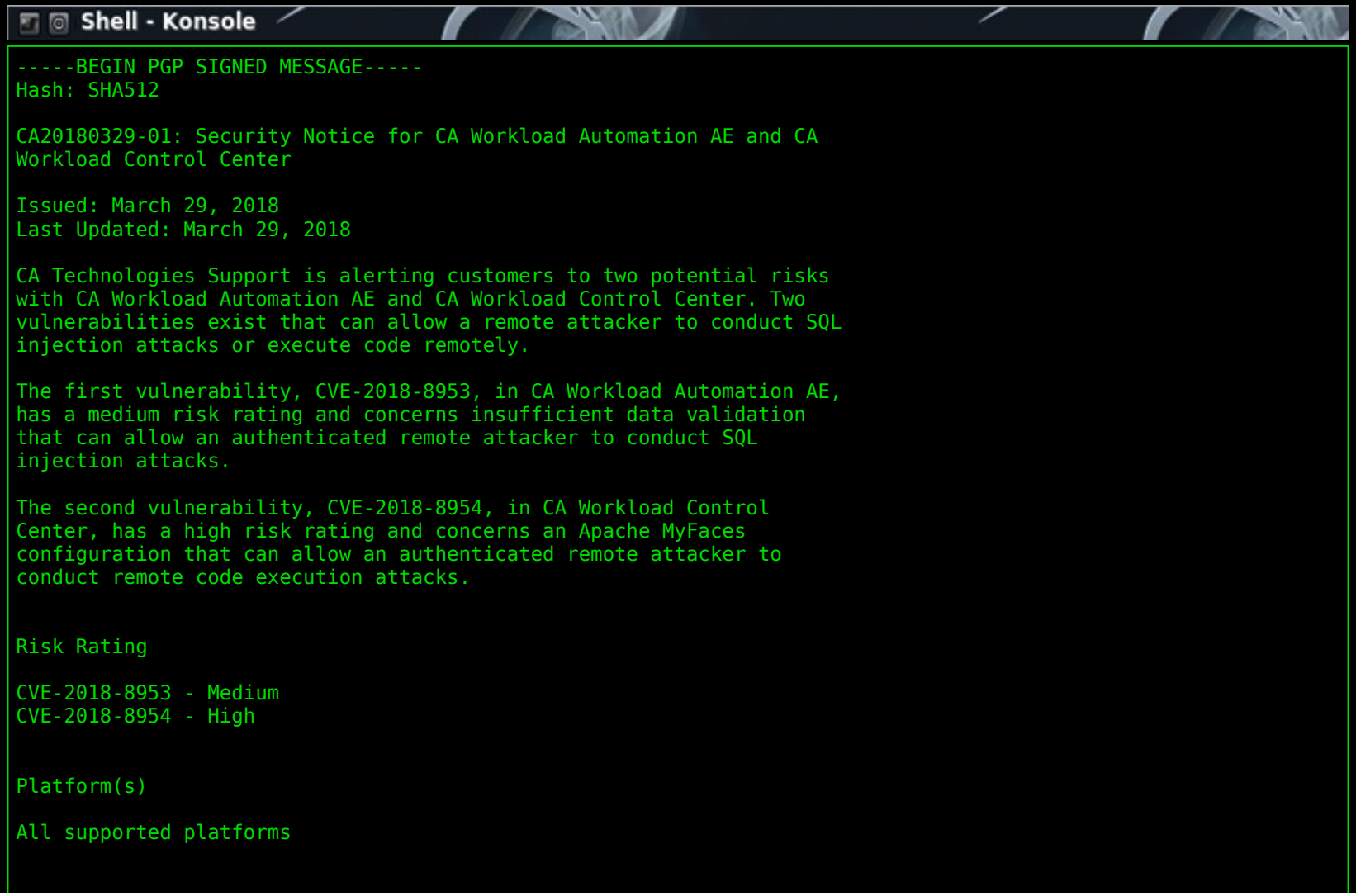
March 30, 2018

Exploit Collector

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 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 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.

Exploit Collector

Download



```
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 r11.3.6:
Apply SP7.

CA Workload Control Center (CA WCC) r11.4 SP5:
Apply patch RO99200 or CA Workload Control Center (CA WCC) r11.4 SP6


References
```

```
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: Initial Release


Customers who require additional information about this notice may
contact CA Technologies Support at https://support.ca.com/

If you discover a vulnerability in CA Technologies products, please
send a report to CA Technologies Product Vulnerability Response
at vuln <AT> ca.com

Security Notices and PGP key
support.ca.com/irj/portal/anonymous/phpsbpldgpg
www.ca.com/us/support/ca-support-online/documents.aspx?id=177782


Regards,

Regards,
Ken Williams
Vulnerability Response Director
CA Technologies Product Vulnerability Response Team

Copyright (c) 2018 CA. 520 Madison Avenue, 22nd Floor, New York, NY
10022.  All other trademarks, trade names, service marks, and logos
referenced herein belong to their respective companies.

-----BEGIN PGP SIGNATURE-----
Version: Encryption Desktop 10.3.2 (Build 16620)
Charset: utf-8

wsFVAwUBWr2G/8Mr2sgsME5lAQoYsQ//Tt/AFWC716QPLJLhQtdwIkMuD1xjEjeM
VXnLjDxakia0czUXWKkvL44O8SINlhPqgu0PJe7soGTvq1AqSO1BlX5nTSlcz0lS
3IWj3CZQnGIx15blX6nfWAdIO8mwH7Yxc/FtG2QT3AmjuJW+C9sxAljcCv9fK2Rk
dY9om/tSmCXYwfuy/z4jpEqRXZLyOhYQ9P3+32oWSJeD4xSnifcUxbtLvm3urI9o
es14hVTL4fnX2/E33hK1ndNRuQaGuGz0oy5xLWhJ8MmkDK404tZnATRvwH5jLASY
```

```
/Tc8wpW3SLh8MrEONN++VeCtUhuWAwnCqx/fA8JCGWYEfjp7WXlGMgArWNRc1WmD
tfPwcRGax7A=
=mX47
-----END PGP SIGNATURE-----
```

Source: packetstormsecurity.com

Related Posts

Exploit Collector

Popular Posts

Linux/x86 Read /etc/passwd Shellcode

62 bytes small Linux/x86 read /etc/passwd shellcode.

Exploit Collector

Microsoft Internet Explorer VBScript Engine CVE-2018-8174 Arbitrary Code Execution Vulnerability

Microsoft Internet Explorer is prone to an unspecified arbitrary code-execution vulnerability.

Attackers can exploit this vulnerability to execute arbitrary code in the ...

WhatsApp 2.18.31 iOS Memory Corruption

WhatsApp version 2.18.31 on iOS suffers from a remote memory corruption vulnerability.

Archive

Exploit Collector