Security Vulnerability Alert

A significant security vulnerability risk has been identified with computer processors that have been recently highlighted in the news. The hardware vulnerability is known as the "speculative execution side-channel attacks" affecting most modern processors and operating systems, including Intel, AMD, IBM, ARM, Microsoft and Apple. CGC has reviewed all available documentation and discussed recommendations with our software and hardware vendors/partners. Collectively, we have identified that the eCMS platforms are all affected by this vulnerability–IBM iSeries, Microsoft Windows and Apple IOS platforms.

The following link provides specific information about the vulnerability: https://meltdownattack.com/

This vulnerability is considered medium risk. The vulnerability was discovered by a technical team, and to date, no virus or malware have been identified exploiting this issue.

Hosted Customers:

CGC has already started deploying updates to our hosted environment to address this vulnerability. We will be staging the appropriate PTFs to the IBM iSeries systems over the next three weekends, and will be applying the hardware firmware updates during the February 9, 2018 maintenance weekend. CGC expects to have all systems updated and the risk mitigated by the middle of February 2018.

On-premise Customers:
Customers with on-premise implementations should review the below items and take the appropriate course of action for their organizations.

IBM iSeries Platform
iSeries hardware and operating system software require updates to address this vulnerability. Please review the below IBM provided links and identify the fix for your hardware and software levels. For customers with Tech Agreements, please schedule your IBM support resource to perform your firmware update. Once the firmware update is completed, please open an incident to schedule CGC to install the OS updates.
Hardware Firmware Updates
OS Software Updates

Windows Platform
The Intel processor hardware that supports the Windows OS is affected. The firmware on these computers needs to be updated to address the vulnerability. This includes all server, desktop and tablet computers. Please contact your hardware vendor for the appropriate firmware update for your systems. The Windows Operating Systems should install the update automatically via Windows update. The following link provides detailed information regarding the Microsoft requirements.
https://www.kb.cert.org/vuls/id/AAMN-AUP5VG

IOS Platform
Apple has released multiple security updates for their IOS devices. Please review and update your devices accordingly.
https://www.us-cert.gov/ncas/current-activity/2017/10/31/Apple-Releases-Multiple-Security-Updates