January 8, 2018

Dear CA Customer:

The purpose of this Advisory is to update the **IMPACT** statement for advisory AAPIGTW-100549 that informed you of a potential problem that has been recently identified with **CA API Gateway**. Please read the information provided below and follow the instructions in order to avoid being impacted by this problem.

**PRODUCT(S) AFFECTED:** CA API Gateway **RELEASE:** 8.0 thru 9.3

**PROBLEM DESCRIPTION:**

CVE-2017-5754, CVE-2017-5753, and CVE-2017-5715 have been recently identified in industry-wide "multiple microarchitectural (hardware) implementation issues affecting many modern microprocessors, requiring updates to the Linux kernel, virtualization-related components, and/or in combination with a microcode update."

Ref: <https://access.redhat.com/security/vulnerabilities/speculativeexecution>

**SYMPTOMS:**"An unprivileged attacker can use these flaws to bypass conventional memory security restrictions in order to gain read access to privileged memory that would otherwise be inaccessible. There are 3 known CVEs related to this issue in combination with Intel, AMD, and ARM architectures. Additional exploits for other architectures are also known to exist. These include IBM System Z, POWER8 (Big Endian and Little Endian), and POWER9 (Little Endian)."

Ref: https://access.redhat.com/security/vulnerabilities/speculativeexecution

**IMPACT**:
On-premise CA API Gateway distribution versions are impacted by this issue.

**WORKAROUND**:
There is currently no known workaround for this issue.

**PROBLEM RESOLUTION:**

CA has issued an expedited Monthly Platform Patch for the API Gateway which is strongly advised that customers apply to all APIM Portals in their environment. You can download the latest monthly platform patch from the CA API Management Solutions & Patches page at <https://www.ca.com/us/support/ca-support-online/product-content/recommended-reading/technical-document-index/ca-api-management-solutions-and-patches.aspx>

Additionally, customers are advised to apply vendor-provided patches to hardware that is being used to run the Virtual Appliance, Container, or Software form factors as they become available.

If you have any questions about this Advisory, please contact CA Support.

Thank you,

CA Support Team