Proactive Notification: Advisory

Dear CA Customer:

The purpose of this Critical Alert is to inform you there is no known product specific impact to **CA Advanced Authentication, CA RiskMinder Products.** Please read the information provided below and follow the vendor instructions as needed to avoid being impacted by this problem.

PRODUCT(S) AFFECTED: CA Advanced Authentication, CA RiskMinder Release: 8.0 thru 9.0.01

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

Ref: https://support.microsoft.com/en-au/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution

Ref: https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-vulnerabilities-in

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)."

Proactive Notification: Advisory

Impact:

There is no known product specific impact to **CA Advanced Authentication, CA RiskMinder**.

WORKAROUND:

There is no known workaround for this issue.

PROBLEM RESOLUTION:

Patches are currently being released by affected vendors.

In the event of an issue with **CA Advanced Authentication, CA RiskMinder** after applying a vendor specific patch, CA will work with the vendors to ensure a quick resolution.

All current and new releases will be tested with the vendor patched systems of **CA Advanced Authentication, CA RiskMinder** .

As more information becomes available from vendors, CA will issue additional notifications to advise customers as needed.

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

Thank you,

CA Support Team

Copyright © 2017 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

To unsubscribe from this service, please follow the link below:
https://support.ca.com/irj/portal/hyperSubscription