Service Bulletin

Security Advisory

No. 20180214-5715/ Revised February 14, 2018

Allworx® hardware products have no Meltdown and Spectre vulnerabilities; software products on shared platforms may require administrator attention

Revision 1.0
Last Updated February 14, 2018
For Public Release February 14, 2018

Summary

Allworx has reviewed the details of the Meltdown and Spectre vulnerabilities (CVE-2017-5715, CVE-2017-5753, and CVE-2017-5754) and has determined that all Allworx server and IP phone products are not vulnerable. These exploits require malicious third-party software to execute on the platform in question, and Allworx servers and IP phones have no provisions to allow such a condition to exist.

Allworx software applications on the Windows platform, such as Allworx Interact™, OfficeSafe™, and View™, do not introduce or increase the risk of vulnerability to Meltdown and Spectre, as these attacks are directed at the platforms on which these applications run and not the actual applications. Customers who run these applications on dedicated hardware have no vulnerability, as Meltdown and Spectre are not remotely exploitable. It is the responsibility of the platform administrator/owner to ensure that proper protections have been applied (e.g., operating system patches). The "Recommended Next Steps" section listed below includes relevant links for protecting your applications from compromises of their hypervisor, from process-to-kernel attacks, or from process-to-process attacks.

The Allworx Portal operates on a cloud-based service, and Allworx is working with this service to ensure that all appropriate mitigations are being considered and implemented.

Allworx Reach™ for Android and Allworx Reach for iOS are dependent on Google and Apple, respectively, for operating system patches. Allworx recommends installing the mobile device manufacturers' operating security updates promptly. The Meltdown and Spectre vulnerabilities are not remotely exploitable, so the threat to information stored by the Reach mobile app would require installation of a hostile app. Therefore, restrictions or self-control regarding third-party app installation reduces risk.

- Google Android patches in December 2017 and January 2018 contain some mitigations. Google recommends the security patch level of at least 2018-01-01. Notably, however, many manufacturers do not promptly update and distribute Android operating system software.
- Apple mitigations were published as iOS 11.2 updates in January.

Affected Products

Products that run on platforms that may require some attention from system administrators

- Allworx Interact
- Allworx OfficeSafe
- Allworx View
- Allworx Reach for Android
- Allworx Reach for iOS

Products Not Vulnerable

- Allworx servers
- Allworx IP phones
- Allworx Portal web site

Additional Details

Meltdown and Spectre are exploits which allow a program on the same system to read data that it should not be allowed to access.

- **CVE-2017-5715**

  Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
- **CVE-2017-5753**

  Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
- **CVE-2017-5754**

  Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache.

Additional details about these vulnerabilities may be found at https://spectreattack.com/.

Recommended Next Steps

Sites concerned about these or other vulnerabilities should:

- Regularly update the Allworx System Software to the most recent version available on the Allworx portal
- Consider dedicated hardware to run View or Interact applications, or:
- Ensure that Allworx applications running on a cloud or virtualized platform have secured hypervisors, for example:
    - VMware:
        - https://kb.vmware.com/s/article/52245
        - https://www.vmware.com/us/security/advisories/VMSA-2018-0002.html
    - Amazon Web Services:
        - https://aws.amazon.com/security/security-bulletins/AWS-2018-013/
    - Azure:
        - https://azure.microsoft.com/en-us/blog/securing-azure-customers-from-cpu-vulnerability/
    - Google Cloud Platform:
        - https://www.blog.google/topics/google-cloud/answering-your-questions-about-meltdown-and-spectre/
    - Microsoft: (including links to OEM hardware vendor firmware updates)
        - https://support.microsoft.com/en-us/help/4073757/protect-your-windows-devices-against-spectre-meltdown
- Ensure that Allworx applications running on cloud, virtualized, or multi-user (Remote Desktop Services, Terminal Server, *etc*) platforms have operating system updates to mitigate process-to-kernel attacks, or from process-to-process attacks:
    - https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution
    - http://windows.microsoft.com/en-us/windows7/install-windows-updates
- On mobile devices, install the latest operating system and security updates (iOS 11.2, Android with security patch 2018-01-01). See:
    - Android Security Bulletin https://source.android.com/security/bulletin/2018-01-01
    - Apple Security Update https://support.apple.com/en-us/HT201222
- A thorough inventory of mitigating patches from many vendors is available at:
    - https://github.com/hannob/meltdownspectre-patches

Revision History

Revision 1.0	February 14, 2018	Initial public release