Written by Alice Marshall
23 February 2018

Security and risk management leaders must take a pragmatic and risk-based approach to dealing with Spectre and Meltdown, Gartner says-- after all, not all software and processors are vulnerable to the threats in the same way.

"[T]he risk will vary based on the system's exposure to running unknown and untrusted code," the analyst continues. "The risk is real, but with a clear and pragmatic risk-based remediation plan, security and risk management leaders can provide business leaders with confidence that the marginal risk to the enterprise is manageable and is being addressed."

Gartner offers 7 steps security leaders can take to mitigate the risk Spectre and Meltdown pose:

1. Modern OSs and hypervisors depend on structured, layered permission models to delivery security isolation and separation. Since the exploitable design implementation is in hardware (below the OS and hypervisor) all software layers above are affected and vulnerable. However since memory can only be read, not altered, exploiting the flaw requires the introduction and execution of untrusted code on the target system, which is difficult on a well-managed server or appliance. As such, one should not rush to "panic patch," as some early patches have had conflicts with security systems, while others hit performance.
2. Nearly every modern IT system will be affected, to some extent-- be it desktops, mobile devices, servers, virtual machines, network and storage appliances, operation technology and IoT devices. All require a deliberate, phased plan of action for remediation efforts. A first step should involve an inventory of affected systems, with each system getting a detailed database or spreadsheet tracking the device or workload, microprocessor version, firmware version and OS.
3. Spectre and Meltdown are not remotely exploitable. A successful attack requires the execution of code on the system. As such, application control and whitelisting on all systems reduces the risk of unknown code execution. However IaaS infrastructure remains vulnerable until cloud providers update the underlying firmware and hypervisor layer.Strong separation of

duties (SOD) and privileged account management (PAM) further reduce the risk of introduction of untrusted code.

4. Break down a remediation strategy into prioritised phases, because the risk, performance implications and potential hardware upgrades required will vary greatly among use cases. Start with the systems most at risk, namely desktops, virtual desktop infrastructure (VDI), smartphones and externally facing servers.

5. Security leaders must be prepared for scenarios where the appropriate decision is not to patch. Some cases involve older systems lacking in patches, others have the performance impact not offset by the reduction in risk. Even some well-managed servers might not be patched in order to protect performance. However Gartner still recommends patching and firmware upgrades in the case of server workloads where the performance characteristics allow.

6. Multiple mitigating controls can reduce risk in the case of non- or partially-patched systems. The single most important issue to address is restricting the placing of unknown or untrusted code onto the device. A "default deny" approach is required, together with application control and whitelisting. Traditional endpoint protection platforms and network-based intrusion prevention systems should also mitigate risk.

7. Spectre and Meltdown represent a new class of vulnerabilities, and this is just the beginning. The underlying exploitable implementation will remain for years to come.

"Ultimately, the complete elimination of the exploitable implementation will require new hardware not yet available and not expected for 12 to 24 months. This is why the inventory of systems will serve as a critical roadmap for future mitigation efforts," Gartner concludes. "To lessen the risk of future attacks against vulnerabilities of all types, we have long advocated the use of application control and whitelisting on servers. If you haven't done so already, now is the time to apply a default deny mindset to server workload protection — whether those workloads are physical, virtual, public cloud or container-based. This should become a standard practice and a priority for all security and risk management leaders in 2018."

Go Gartner Provides 7 Steps Security Leaders Can Take to Deal With Spectre and Meltdown