Falla nei processori, 7 consigli per contrastare le vulnerabilità Spectre e Meltdown

Spectre e **Meltdown** sono i nomi in codice che sono stati dati a diversi ceppi di un nuova classe di attacchi informatici, individuati nel gennaio 2018, che mirano la vulnerabilità della maggior parte dei chip di computer prodotti negli ultimi 20 anni.

Attraverso uno studio condotto dall'azienda americana **Gartner Inc,** multinazionale operante nella consulenza strategica, ricerca e analisi nel campo dell'Information Technology, i leader della sicurezza e della gestione del rischio devono adottare un approccio pragmatico e basato sul rischio per le minacce in corso poste da questa nuova classe di vulnerabilità.

"*Il rischio è reale, ma con un piano di bonifica chiaro e pragmatico basato sul rischio, i responsabili della sicurezza e della gestione del rischio possono fornire ai leader aziendali la certezza che il rischio marginale per l'azienda è gestibile e viene affrontato*" –ha affermato **Neil MacDonald**, vicepresidente, di **Gartner**.

Ma prima andiamo con ordine, spieghiamo cosa intendiamo quando parliamo di Meltdown e Spectre.

Meltdown

È la falla che interessa computer desktop, portatili e sistemi

cloud che utilizzano diverse generazioni di processori **Intel**, prodotti a partire dal 1995 (sembra facciano eccezione le versioni Itanium e Atom, ma solo se prodotte prima del 2013). Per ora i ricercatori hanno la certezza che la falla riguardi Intel, mentre sono ancora in corso verifiche per accertarsi se siano coinvolti anche processori di altre marche e con architetture diverse come ARM e AMD.

Spectre

I ricercatori stimano che "praticamente tutti i sistemi" siano affetti da Spectre, quindi: computer desktop, portatili, server cloud e smartphone. Il problema riguarda i processori Intel, **AMD** e **ARM**. L'estensione della falla sembra quindi essere molto maggiore e per gli esperti di sicurezza le prospettive non sono incoraggianti, considerato che una soluzione software per questo problema richiede un approccio articolato, quindi più tempo.

L'azienda ha identificato sette passaggi che i responsabili della sicurezza possono attualmente adottare per ridurre i rischi:

1. **Riconosci il rischio, ma non farti prendere dal panico**

I moderni sistemi operativi (OS) e gli hypervisor dipendono da modelli di autorizzazione strutturati e stratificati per garantire l'isolamento e la separazione della sicurezza. Poiché questa implementazione di progettazione sfruttabile è sull'hardware, sotto il sistema operativo e l'hypervisor, tutti i livelli software sopra sono interessati e vulnerabili. Tuttavia, la memoria può essere solo letta, ma non modificata. Lo sfruttamento del difetto richiede che il codice non sicuro sia introdotto ed eseguito sul sistema di destinazione, il che dovrebbe essere estremamente difficile su un server o

un’appliance ben gestiti come una rete o un’appliance di archiviazione. C’è anche un vantaggio nel non ricorrere alla “patch di panico”. Le patch iniziali creavano conflitti con alcune offerte antivirus e bloccavano i computer **Windows**.

2. **Fai un inventario dettagliato**

Quasi tutti i moderni sistemi IT saranno interessati in una certa misura. Dal momento che Y2K ha una vulnerabilità interessata, molti sistemi (desktop, dispositivi mobili, server, macchine virtuali, appliance di rete e di archiviazione, tecnologia operativa e dispositivi di Internet of Things) hanno richiesto un piano di azione pianificato e deliberato per gli interventi di riparazione. Il punto di partenza per i responsabili della sicurezza deve essere un inventario dei sistemi interessati. In alcuni casi, la decisione appropriata per il rischio sarà quella di non applicare la patch. Per ciascun sistema, è necessario un database dettagliato o un foglio di calcolo per tenere traccia del dispositivo o del carico di lavoro, della versione del suo microprocessore, della versione del firmware e del sistema operativo.

3. **Sviluppare un piano di rimedio prioritario**

Le vulnerabilità non sono direttamente sfruttabili da remoto. Un attacco di successo richiede che l’attaccante esegua il codice sul sistema. Pertanto, il controllo dell’applicazione e la whitelist su tutti i sistemi riducono notevolmente il rischio di esecuzione di codice sconosciuta. Tuttavia, l’infrastruttura condivisa come infrastruttura di servizio è particolarmente vulnerabile fino a quando i provider di cloud non aggiornano il loro firmware e il livello hypervisor sottostante (che i principali provider hanno fatto).

4. **Dare priorità agli sforzi di rimedio**

Quando si escogita una strategia di correzione, si consiglia di suddividere la strategia in fasi prioritarie, poiché il

rischio, le implicazioni sulle prestazioni e i potenziali aggiornamenti hardware richiesti variano notevolmente tra i casi d'uso. Inizia con i sistemi che rappresentano il maggior rischio – computer, virtual desktop infrastructure **(VDI)**, smartphone e server rivolti all'esterno.

5. **Riconoscere che a volte la decisione appropriata e basata sul rischio non deve essere applicata**

I responsabili della sicurezza devono essere preparati per scenari in cui la decisione appropriata potrà essere quella di non applicare le patch. In alcuni casi, ciò sarà dovuto alla mancanza di patch sui sistemi più vecchi. In altri casi, l'impatto sulla performance non viene compensato dalla riduzione del rischio, quindi le patch non verranno applicate. Anche per alcuni server ben gestiti, è possibile decidere di rinunciare alle patch per proteggere le prestazioni fino a quando le patch future avranno impatti accettabili. Tuttavia, per i carichi di lavoro del server, quando le caratteristiche delle prestazioni lo consentono, si consiglia di aggiornare patch e firmware.

6. **Non inserire codici sconosciuti nei dispositivi**

Per i sistemi che non sono riparati o solo parzialmente riparati, più controlli attenuanti possono ridurre il rischio. Il problema più importante da affrontare è limitare la possibilità di inserire un codice sconosciuto o non attendibile sul dispositivo. Riducendo questo, i rischi sono significativamente ridotti, poiché gli attacchi richiedono l'esecuzione di codice locale.

7. **Pianificare ulteriori sforzi di riduzione del rischio nei prossimi anni**

Spectre e Meltdown rappresentano una nuova classe di vulnerabilità, e questo è solo l'inizio. *"In definitiva, l'eliminazione completa dell'implementazione sfruttabile richiederà un nuovo hardware non ancora disponibile e non*

previsto per 12 a 24 mesi, motivo per cui l'inventario dei sistemi fungerà da roadmap fondamentale per i futuri sforzi di riduzione del rischio", ha affermato MacDonald. "Se *questi carichi di lavoro sono fisici, virtuali, cloud o pubblici ciò dovrebbe diventare una pratica standard e una priorità per tutti i leader della sicurezza e della gestione dei rischi nel 2018. "*

> *Falla nei processori, 7 consigli per contrastare le vulnerabilità Spectre e Meltdown*