Spectre e Meltdown, due bug di sicurezza che sconvolgono il mondo dell'informatica

Meltdown e Spectre stanno facendo parlare molto di sé in queste ore: i due bug coinvolgono in maniera diversa i processori, con il secondo che è presente su tutte le CPU sul mercato. Un bel grattacapo per cui non esistono soluzioni definitive

Il settore dell'informatica e dell'elettronica è in subbuglio: due nuove vulnerabilità, scoperte qualche mese fa ma rese pubbliche in questi giorni, stanno scuotendo il settore dalle fondamenta. **Meltdown** e **Spectre** - questi i nomi delle vulnerabilità - vanno infatti a colpire dei difetti di progettazione dell'hardware, non sempre risolvibili e a volte a caro prezzo.

Meltdown

Meltdown è la **vulnerabilità scoperta nei processori Intel** di cui abbiamo avuto modo di parlare già negli scorsi giorni. Un **errore di progettazione nella gestione della memoria virtuale** fa sì che sia possibile accedere all'area di memoria dedicata al kernel, di fatto aprendo le porte ad attacchi che permettono di leggere dati di ogni tipo in memoria.

Oltre ai processori Intel, uniche vittime nel panorama x86, anche alcune versioni dell'archiettura ARM ne soffrono: anche i **Cortex-A15**, **Cortex-A57** e **Cortex-A72** infatti **sono vittima** di questa vulnerabilità. C'è una piccola differenza, nel senso che, al posto dei segmenti di memoria riservati, sono i registri protetti a essere accessibili dai processi utente.

La buona notizia è, però, che **Meltdown è risolvibile via software**, sebbene con un decremento a volte sostanziale delle prestazioni. Tutte le principali piattaforme (Linux, Windows, macOS) hanno già ricevuto o stanno per ricevere un aggiornamento che mitiga il problema.

Si tratta di un bel grattacapo per Intel, che è stata costretta a correre velocemente ai ripari. L'azienda ha cercato di difendersi affermando che "non c'è un bug nei processori e tutto funziona come previsto": è vero, ma il problema sta proprio nel fatto che il funzionamento regolare del processore espone i dati ad attacchi e la difesa non poggia quindi su solide basi. L'azienda dovrà quindi **riprogettare i propri processori** per tenere conto di questa vulnerabilità, mentre i possessori dei processori prodotti finora dovranno convivere con un calo delle prestazioni.

Spectre

Discorso differente, invece, riguarda **Spectre**. Si tratta di una vulnerabilità simile a Meltdown, ma potenzialmente **molto più grave**: **Spectre non è infatti risolvibile con una patch o con un intervento software**. Il problema è simile a quello da cui deriva Meltdown, ma **coinvolge tutti i processi in esecuzione sul sistema e non solo il kernel**.

Il problema nasce con l'**esecuzione fuori ordine** (*out-of-order execution*) delle istruzioni: l'esecuzione *out-of-order* prevede che il **processore faccia delle scommesse** su quale sarà il codice che dovrà andare a eseguire e lo esegua. Il vantaggio teorico di questo approccio sta nel fatto che **l'alternativa è che il processore non faccia nulla**, in attesa che le istruzioni vengano caricate dalla memoria. L'obiettivo è infatti quello di **tenere la pipeline sempre piena** in maniera tale da ottimizzare l'uso del processore e ottenere le migliori prestazioni possibili. Anche se il processore perde la sua scommessa ed esegue istruzioni sbagliate, non c'è - almeno teoricamente - alcun impatto negativo.

Quello che si è scoperto, però, è che questo non è vero: se l'impatto negativo non c'è dal punto di vista prestazionale, c'è dal punto di vista della sicurezza. Il processore, infatti, in buona sostanza **non esegue i dovuti controlli di sicurezza sul codice che va a eseguire e non elimina ogni traccia di quanto prodotto da una scommessa sbagliata**. Questo consente, con un processo sufficientemente complesso, di leggere informazioni nei segmenti di memoria di altri processi o di ricavare informazioni dalla memoria del processo stesso.

Se il primo caso apre a scenari abbastanza facili da immaginare, come la **lettura di password o chiavi di cifratura nella memoria di altri processi**, il secondo è particolarmente significativo per quei processi che eseguono codice non sempre controllato, come i **browser**. L'esempio principe è proprio quello dei browser: a causa di Spectre, **un ipotetico script in JavaScript potrebbe avere accesso ai cookie di login di altri siti**. Va da sé che questo sia causa di problemi potenzialmente enormi.
Questo aspetto è ancora più accentuato nel caso delle **virtual machine**: **del codice eseguito in una macchina ospite potrebbe infatti arrivare a leggere la memoria della macchina ospitante**, di fatto accedendo a informazioni presenti sia sulla macchina fisica che su altre macchine ospiti.
Quest'ultimo aspetto è particolarmente preoccupante per i **fornitori di servizi di hosting o di cloud computing**, che dovranno essere particolarmente proattivi con le contromisure software.

Spectre e Meltdown: le soluzioni

Proprio le contromisure sono l'aspetto più significativo di Spectre, perché fondamentalmente sono **poche e non centralizzate**. Oltre a **correzioni nei sistemi operativi e nel microcodice dei processori**, infatti, la maggioranza delle correzioni dovranno arrivare nei singoli software, che **dovranno essere ricompilati** per tenere in conto la possibilità di attacco tramite Spectre. Non si tratta, però, di soluzioni definitive che eliminano il problema, ma di tentativi di arginare il problema. **Tutti i processori sono coinvolti**: Intel, AMD e ARM sono impegnate a sviluppare delle pezze. AMD afferma che i suoi processori sono immuni alla lettura dei dati dal kernel e sono vulnerabili in alcuni casi specifici alla lettura di dati nella memoria dei processi.
Quello che colpisce è il fatto che uno dei più diffusi concetti nella progettazione delle architetture dei processori si sia ora rivelata causa di grossi problemi di sicurezza. Tutti i processori x86 degli ultimi 20 anni - dopo il primo Pentium e a esclusione degli Itanium e degli Atom pre-2003) - sono vulnerabili a questo attacco, segno che il problema è di tipo strutturale e progettuale. L'unica vera soluzione a questo problema sarà un **cambiamento nelle architetture**, ma il fatto che non sia realmente possibile eliminare del tutto il rischio lascia miliardi di dispositivi potenzialmente a rischio.
Sono al momento in fase di rilascio **aggiornamenti** per Windows, macOS e Linux, con i principali browser (Chrome, Firefox, Edge, Safari) che seguono a ruota e stanno ricevendo o riceveranno aggiornamenti. Entro la fine della prossima settimana, Intel stima che il 90% dei dispositivi con processori degli ultimi 5 anni saranno protetti. **È quindi importante tenere monitorati i messaggi che propongono aggiornamenti ed eseguirli.** Intel e AMD proporranno aggiornamenti del microcodice da installare tramite aggiornamenti appositi.
L'aspetto positivo - per così dire - di Spectre è che sembra attualmente essere **molto difficile da sfruttare**. Non sembra possibile, stando alle conoscenze attuali, portare avanti attacchi su larga scala che minino la sicurezza dei nostri sistemi alle fondamenta, e l'eventualità di essere colpiti in quanto singoli utenti appare ora ridotta.
Ciò, però, non deve trarre in inganno. **Non si tratta di problemi di importanza secondaria o di eventualità remote che possono essere trascurate**; in questo caso, l'allarmismo sembra giustificato dalla gravità dei problemi. **Installare gli aggiornamenti che mitigano le problematiche è essenziale** per poter utilizzare senza preoccupazioni (o quasi) prodotti collegati alla Rete, poiché il rischio è quello di **lasciare accesso a informazioni riservate come dati bancari, password e così via**. Rischi concreti, reali e che possono coinvolgere ciascuno di noi. Così come le porte blindate non possono garantire al 100% che i ladri non entrino in casa, così anche le patch sviluppate non possono garantire la totale immunità da questi problemi; tuttavia, sapendo che i ladri potrebbero entrare in casa, chi lascerebbe solo una banale porta di legno - per di più aperta - a guardia della propria casa?

di Riccardo Robecchi pubblicata il 05 Gennaio 2018, alle 17:24 nel canale Sicurezza Intel AMD ARM