Intel: grave falla sulle CPU, fix pronto e distribuito

Dopo la notizia di **MINIX**, l'OS installato su CPU **Intel** di ultima generazione, che ha accesso a informazioni importanti a nostra insaputa, nelle ultime 48 ore **The Register**, ne ha scoperto un nuovo bug sulle. Così riferisce **AMD**:

«L'esecuzione speculativa del bug sul kernel a livello hardware è da incolpare a Intel; non può essere fixato utilizzando un aggiornamento del microcode e richiederà una patch a livello KPTI per tutti gli OS colpiti.»

Prima di entrare in altri dettagli, una spiegazione sul problema: il bug è stato scoperto a livello hardware e riguarda un ***exploit*** che è in grado di garantire l'accesso a livello del kernel da malintenzionati. Dal momento che questo esiste a livello hardware, una patch tramite ***microcode*** non è apparentemente possibile. L'unica soluzione nota è intervenire tramite il sistema operativo, che richiederebbe una riprogettazione del l'OS stesso, su cui **Windows**, **Linux** e **Apple** hanno già lavorato.
Microsoft ha già rilasciato una patch per i propri sistemi Windows 10, con il codice **KB4056892**. Comunque, il problema è che qualsiasi patch potrebbe introdurre una **penalità temporale cruciale per il sistema**, il ché significa che in alcuni casi le CPU potrebbero **rallentare drasticamente**. Abbiamo visto numeri quotati fino al **30%**, ma le stime approssimative indicano un rallentamento di circa il **17%**. Quindi, qual è esattamente il problema?
Prima di entrare nei dettagli, ecco la dichiarazione di **AMD**, che fondamentalmente ha dato più dettagli su quale sia il problema:

> **«I processori AMD non sono soggetti ai tipi di attacchi a livello kernel. La microarchitettura AMD non consente riferimenti di memoria, inclusi riferimenti speculativi, che accedono a dati con privilegi più elevati quando vengono eseguiti in una modalità con privilegi minori quando tale accesso comporterebbe un errore di pagina.»**

Dato che Intel ha parlato a lungo di questo problema, possiamo dedurre abbastanza facilmente da questa affermazione che il problema ha a che fare con riferimenti speculativi nei processori Intel. L'esecuzione speculativa è fondamentalmente una forma di ***preemption*** che cerca di prevedere quale codice verrà eseguito, quindi lo preleva e lo esegue prima che l'ordine effettivo arrivi. Quindi si dovrebbe avere un kernel assolutamente pronto per ogni comando, invece di lasciarlo aspettare.
Il problema, come risulta dai commenti di AMD, è che è possibile sfruttare questa funzione per eseguire in modo speculativo un codice che normalmente verrebbe bloccato, finché si interrompe l'esecuzione effettiva del codice prima che sia possibile eseguire un controllo. Questo significa che un utente di **livello 3** può leggere i dati del kernel di **livello 0** utilizzando l'esecuzione speculativa, poiché il controllo dei privilegi non verrà effettivamente attuato finché il codice non viene eseguito sul main.
Il ***layer* Kernel** è attualmente presente nello spazio di indirizzamento della memoria virtuale di tutti i processi per garantire una consegna rapida durante l'esecuzione del codice, ma è completamente invisibile a tutti i programmi. Il kernel proverà fondamentalmente a prevedere quale codice verrà eseguito successivamente e quando un programma effettua una chiamata di sistema a esso, sarà già pronto per la consegna. Ciò può aumentare significativamente i tempi di esecuzione ma, rappresenta anche un fastidioso errore di sicurezza poiché nessun controllo dei privilegi è presente allo stadio del kernel. L'unico modo per aggirare questa caratteristica di livello hardware è usare quella che

viene chiamata una tecnica ***Kernal Page Table Isolation*** (***KPTI***) che renderà il kernel completamente cieco al sistema e lo rimuoverà dallo spazio di memoria virtuale, fino a quando non si verificherà una chiamata di sistema. Inutile dire che questo potrebbe introdurre severe penalità nel tempo in situazioni di commutazione di contesto in cui sono richieste molte chiamate di sistema. Il team di Linux ha anche rimuginato su ***FUCKWIT*** (**Forcefully Unmap Complete Kernel with Interrupt Trampolines**) che dovrebbe dare un'idea di quanto sia frustrante il bug per gli sviluppatori.
Secondo alcune fonti, questo numero può variare dal **5%** al **30%** a seconda del tipo di processore in uso, poiché le moderne CPU hanno una funzionalità denominata **PCID** che può ridurre l'impatto sulle prestazioni. Secondo una soluzione KPTI esistente pubblicata su ***Postgresql***, ci si dovrebbe aspettare un rallentamento del caso migliore del **17%** e un rallentamento del **23%** nel caso peggiore. In ogni caso, tutte le fonti concordano sul fatto che un rallentamento si verificherà quasi sicuramente e questo non è qualcosa che Intel può semplicemente applicare a un microcodice. I processori AMD in questo momento non sono interessati dal momento che non utilizzano l'esecuzione speculativa. Quindi la domanda è: chi avrà questo impatto e come questo inciderà sugli utenti finali? La buona notizia per tutti i gamer o utenti "normali" è che non si noterà quasi nessuna differenza una volta applicata la patch poiché i videogiochi e il rendering di base non sono carichi abbastanza pesanti per avere quei rallentamenti. I *client* aziendali come **Google EC2** e **Amazon Compute Engine**, tuttavia, subiranno un drastico impatto dal momento che utilizzano macchine virtuali che possono seriamente compromettere le prestazioni. In secondo luogo, come utente generico, le password e altre informazioni sensibili sono memorizzate nel kernel e questo bug potrebbe potenzialmente garantirne un accesso aperto.
Nelle ultime ore il team di **Phoronix** ha eseguito dei test con KPTI attivo su due CPU, un **Intel Core i7 6800K** e un **Intel Core i7 8700K**; i grafici mostrano un sostanziale degrado di performance che parte dall' **1%** al **53%** nei casi peggiori, ma comunque ciò non comprometterebbe l'utilizzo dei videogiochi.

Il comunicato stampa ufficiale da parte di Intel

Come detto si parla che la patch possa risolvere il problema almeno parzialmente ma a discapito delle prestazioni in modo variabile. Intel però si è subito fatta sentire ed ecco cosa dice nel suo comunicato stampa:

> **«Intel e altre aziende tecnologiche sono state messe a conoscenza di una nuova ricerca di sicurezza che descrive metodi di analisi software che, se usati per scopi dannosi, hanno il potenziale per raccogliere impropriamente dati sensibili da dispositivi informatici che funzionano come progettato. Intel ritiene che questi *exploit* non abbiano il potenziale per corrompere, modificare o eliminare dati. Le recenti notizie secondo cui questi *exploit* sono causati da un "bug" o una "falla", unicamente legati ai prodotti Intel sono scorrette. In base all'analisi fino a questo momento, molti tipi di dispositivi – con processori di aziende differenti e sistemi operativi – sono suscettibili a questi *exploit*. Intel è impegnata nel garantire la sicurezza dei prodotti e dei clienti e sta lavorando a stretto contatto con molte altre aziende tecnologiche tra cui AMD, ARM Holdings e diversi fornitori di sistemi operativi, per sviluppare un approccio a livello industriale per risolvere questo problema in modo rapido e costruttivo. Intel ha iniziato a fornire aggiornamenti software e *firmware* per mitigare questi exploit. Contrariamente ad alcune notizie, qualsiasi impatto sulle prestazioni è legato al carico di lavoro e, per l'utente medio di un PC, non dovrebbe essere importante e sarà mitigato nel tempo. Intel si impegna a seguire le *best practice* industriali nella divulgazione responsabile di potenziali problemi di sicurezza, e per questo motivo Intel e altre aziende avevano intenzione di parlare di questo problema la prossima settimana quando gli aggiornamenti di *software* e *firmware* saranno disponibili. Intel si trova tuttavia costretta a pubblicare questo comunicato in seguito ai report inaccurati dei media. Rivolgetevi al fornitore del sistema operativo o al produttore del sistema e applicate tutti gli**

> **aggiornamenti non appena disponibili. In generale seguire le buone pratiche di sicurezza che proteggono dai malware aiuterà anche a proteggervi dal possibile sfruttamento della falla fino a quando gli aggiornamenti non saranno applicati. Intel ritiene che i suoi prodotti siano i più sicuri al mondo e che, con il supporto dei suoi partner, le attuali soluzioni a questo problema offrano la migliore sicurezza possibile per i propri clienti.»**

Anche se la questione non è per niente conclusa, in attesa di nuovi aggiornamenti, ecco il riassunto di cosa Intel ha detto in modo specifico per capire meglio la situazione:

- Intel ritiene che questi exploit non possono corrompere, modificare o eliminare i dati.
- Intel afferma che non sono solo i suoi prodotti a essere coinvolti. Si parla di prodotti con CPU diverse e sistemi operativi differenti, quindi anche smartphone.
- Intel fa i nomi di **AMD** e **ARM**. Un saggia mossa che sposta l'attenzione, fino ad ora focalizzata sul proprio brand.
- Intel afferma che l'impatto prestazionale per chi usa il PC in modo tradizionale – come la stragrande maggioranza di noi, e quindi per giocare, navigare ecc… sarà di poco conto e sarà mitigato ulteriormente in futuro.
- Intel ritiene che i suoi prodotti siano i più sicuri al mondo.

Test svolti dalla redazione

Abbiamo fatto due semplici ***benchmark*** su lato CPU ovviamente con Windows 10, prima della patch e dopo la patch (KB4056892) per vedere se ci sono dei cambiamenti. Abbiamo usato una CPU Intel Core i5 6600K portato a 4,60 GHz stabili, e come programmi: **Geekbench 4** e **Aida 64**:

Da come si può vedere dai *benchmark* la situazione è cambiata poco e, se i valori su **Geekbench 4** nel prima sono più alto è da attribuirsi a tanti fattori tra cui servizi aperti, cosa stava facendo il PC in quel momento ecc… Su Aida 64 invece alcuni valori sono aumentati, per il motivo descritto prima. Quindi in conclusione, dai primi test nei *benchmark*, si spera in gaming le cose non dovrebbero cambiare. A breve faremo delle verifiche su lato gaming se ci sono cambiamento e aggiorneremo questo articolo, quindi rimanete aggiornati con noi !

Andrew S. Tanenbaum creatore di MINIX scrive una lettera a Intel

Di recente abbiamo parlato dell'**OS** più usato al mondo, **MINIX**, che è installato su gli ultimi processori di **Intel** dal 2008 fino ad oggi.

Intel ME, da quanto si sa, serve per la gestione del PC da remoto e potrebbe anche servire per altre operazioni poco chiare, tanto da indurre associazioni come l'**Electronic Frontier Foundation** (**EFF**) a criticarne apertamente l'uso, avanzando l'ipotesi che si tratti di una **backdoor** mascherata, e sollevando un polverone riguardo la sicurezza; tutto ciò è stato portato alla luce dopo che è stato trovato il modo di hackerare Intel ME tramite porta USB ed è anche per questo che Google ha deciso di rimuovere questa "parte nascosta" delle CPU Intel.
Di tutto ciò, il creatore di MINIX, **Andrew S. Tanenbaum,** pare sia stato all'oscuro, e pare anche che Intel abbia commercializzato un OS che Tanenbaum avrebbe creato nel lontano 1987 a solo

scopo educativo allegato a un proprio libro di testo. Lo stesso Tanenbaum ha inoltre dichiarato che **MINIX 3** è la versione usata per Intel ME alla conferenza ACM SOSP del 2005. Si tratta della prima versione indirizzata ad applicazioni commerciali e Tanenbaum ha spiegato molto in una lettera indirizzata a Intel:

> **«Sapevo che Intel aveva un potenziale interesse in MINIX diversi anni fa quando un componente del vostro team di ingegneri mi ha contattato riguardo un progetto interno segreto e mi ha fatto un sacco di domande tecniche su MINIX, a cui sono stato felice di rispondere [...] Ho avuto un altro indizio quando gli ingegneri hanno iniziato a chiedermi di fare un certo numero di modifiche a MINIX, ad esempio, riducendo l'impatto sulla memoria e aggiungendo #ifdefs intorno ai pezzi di codice in modo che questi potessero essere disattivati staticamente impostando flag nel file di configurazione principale. Un altro indizio è stata la discussione sulla licenza»**

MINIX è stato distribuito sotto licenza **BSD,** senza grandi restrizioni**.** Tanenbaum ritiene che questa sia la ragione principale per cui Intel avrebbe adottato il suo sistema operativo. Nella missiva, Tanenbaum dice di essere rimasto sorpreso e non voler alcun tipo di pagamento o risarcimento da parte di Intel: avrebbe solamente gradito essere stato avvisato.

> **«L'unica cosa che sarebbe stato bello avvenisse è che dopo la conclusione del progetto e la distribuzione del chip, qualcuno di Intel mi avesse avvisato che MINIX è probabilmente il sistema operativo più usato nel mondo sui sistemi x86. Non era certamente richiesto, ma sarebbe stato gentile avvisarmi. Se non altro queste notizie rafforzano la mia opinione che la licenza BSD offre la massima libertà ai potenziali utenti»**

Tanenbaum aggiunge in merito alla non trasparenza di Intel ME e al pericolo che si tratti di una backdoor, che «mettere una presunta spia dentro ogni computer è un mezzo terribile».

MINIX: l'OS più usato al mondo

Quale sistema operativo usate? **Windows**? **Linux**? **Mac OS X**?
Se avete una **CPU Intel** di ultima generazione, sicuramente conterrà un sistema operativo a gestire tanti processi. Il suo nome è **MINIX**. L'OS di **Unix**, originariamente sviluppato da **Andrew Tanenbaum** come strumento didattico per dimostrare la programmazione del sistema operativo, è integrato in ogni nuova CPU Intel. MINIX è in esecuzione sul "**Ring 3**", una parte della CPU non accessibile ai comuni utenti. Il più basso "**Ring**" a cui è possibile accedere è il "**Ring 0**", dove vi è il kernel del sistema operativo installato. La maggior parte delle applicazioni utente si svolgono nel "Ring 3". La prima cosa che si deve quindi pensare è che MINIX (in particolare una versione di **MINIX 3**) è probabilmente la più diffusa distribuzione di **OS** oggi su moderni computer Intel (desktop, laptop e server). Al "Ring 3", come detto, l'utente comune non ha accesso, ma MINIX può accedere completamente all'intero hardware e software dei nostri computer. Conosce tutto e vede tutto, e ciò rappresenta un enorme rischio di sicurezza specialmente nel caso in cui MINIX stia eseguendo molti servizi sul Ring 3 e se non viene aggiornato regolarmente con patch di sicurezza.

Google vuole rimuovere MINIX dai propri server interni

Secondo **Google**, che sta lavorando attivamente per rimuovere il motore di gestione Intel (MINIX) dai propri server interni (per ragioni evidenti di sicurezza), all'interno del Ring 3 esistono le seguenti funzionalità:

- Una lista completa di networking
- File di sistema
- Molti driver (inclusi USB, networking, ecc.)
- Un server web

Esatto, un **server web**. La CPU dispone di un server web segreto e anche qua l'accesso non ci è consentito e, a quanto pare, Intel non vuole che noi utenti comuni sappiamo cosa ci sia dentro e come funzioni.