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 !

Nintendo Switch è la console venduta più velocemente nella storia degli USA

Non è un segreto che **Nintendo Switch** sia un'ottima console, di cui è stato aumentato il valore grazie a ottimi titoli come ***The Legend of Zelda: Breath of the Wild*** e ***Super Mario Odissey*** ma negli USA ha superato le aspettative vendendo così tanto da piazzarsi prima per numero di unità vendute nei primi 10 mesi dal lancio; ha infatti sorpassato il **Wii** vendendo più di 4,8 milioni di console come riportato da **Gematsu**.
A seguire, in classifica abbiamo quindi **Wii** con circa 4 milioni di unità e la **PS4** con 3.95 milioni.

Il presidente di **Nintendo America, Reggie Fils-Aime,** ha dichiarato: «I fan di tutto il paese hanno provato la gioia di poter giocare ai loro giochi preferiti a casa o in viaggio. Ora che molte persone hanno ricevuto **Switch** per le vacanze, cercheremo di portare anche a loro nuove e divertenti sorprese per il 2018.»

Sembra che questo divertimento non mancherà dato il «continuo supporto da grandi aziende come **EA**, **Activsion**, **Ubisoft, Capcom**, **Sega**, **Take 2** e **Bethesda** e un crescente catalogo di contenuti di qualità da sviluppatori Indie» e il sicuro arrivo di ***Kirby: Star Allies***, ***Bayonetta***, ***Bayonetta 2*** e, se i rumor fossero confermati, anche di ***Bayonetta 3***

Un rumor rivelerebbe alcune straordinarie esclusive Xbox

Secondo alcune voci, il 2018 potrebbe essere un anno esaltante per Xbox. In un recente thread su ResetEra, l'utente **Klobrille** – che ha acquisito credibilità dopo aver anticipato notizia come quella del nuovo ***Age of Empires***, del secondo capitolo di ***State of Decay***, riguardo l'ambientazione australiana di ***Forza Horizon 3*** e riguardo la natura MMO-lite di ***Sea of Thieves*** – sostiene che sarebbe in fase di sviluppo un nuovo ***Fable***, sul quale dovrebbe essere al lavoro uno studio britannico, a seguito della chiusura di Lionhead dello scorso anno.

Ci sarebbe poi un nuovo ***Perfect Dark***, su cui sarebbe al lavoro **The Coalition**, sviluppatore di ***Gears of War***, che vedrebbe una Joanna Dark questa volta in terza persona.
Spazio anche per ***Forza Horizon 4***, che uscirà quasi sicuramente entro la fine di quest'anno e che potrebbe essere ambientato in Giappone.
Altre informazioni riguardano infine la co-op della campagna per quattro giocatori in ***Crackdown 3***, il prossimo ***Halo***, che coinvolgerebbe un numero di giocatori "molto alto" (con una probabile modalità **Battle Royale**) e il ritorno di ***Mech Assault***.
Stando a Klobrille, queste informazioni sarebbero state trovate nelle tabelle del database di Microsoft accessibili tramite l'SDK dell'API di Xbox Live e gli utenti della console di Redmond si augurano vivamente che siano vere

---

Svelato il primo trailer per il film Slender Man

Slender Man, noto personaggio di numerosi titoli, nonchè di altrettante leggende metropolitane, arriverà il 18 maggio anche sul grande schermo con il suo film personale, diretto da **Sylvain White**, il cui trailer è stato rilasciato da poco. ***Slender Man*** ci parlerà di una figura misteriosa molto alta con lunghi arti, viso privo di caratteristiche, ritenuto il responsabile di innumerevoli scomparse e suicidi, di bambini e adolescenti, rimanendo fedele alla leggenda originale.

Star Citizen incassa piú di tutti i giochi Kickstarter

Da quanto riportato dal nuovo rapporto di ***Polygon, Star Citizen*** avrebbe raccolto più soldi di tutti i giochi nati grazie alla piattaforma **KickStarter** per il secondo anno consecutivo, facendo il doppio rispetto agli altri titoli nati grazie a questa piattaforma.
Il tanto atteso titolo, nel 2017, è riuscito a raccogliere **34,91 milioni di dollari**, dato però leggermente inferiore rispetto agli incassi fatti nel 2016 che ammontano a circa **36,11 milioni**. Cifre enormi rispetto ad altri titoli KickStarter di successo, i quali, sommando i loro incassi, hanno raggiunto i **17,25 milioni di dollari** nel 2017, e i **17,6 milioni** nel 2016.
Ma ben più importante è che *Star Citizen* sia riuscito in questa impresa nonostante le orde di gente che chiedevano indietro i soldi, costanti ritardi, ed essere citatati a giudizio da **Crytek** per violazione di contratto.

L'ottimismo di Michael Pachter nei confronti di Star Wars Battlefront II

Durante gli ultimi due mesi, si è sentito parlare della polemica sulle *lootbox* in ***Star Wars Battlefront II***. Questo ha avuto un effetto negativo sulle vendite e sulle entrate e costretto l'editore a rivedere le sue proiezioni. Sebbene la controversia abbia indubbiamente influito negativamente sulla performance di EA, l'analista di *Wedbush Securities*, **Michael Pachter**, è convinto che questa sia solo una situazione temporanea e che, dopo la tempesta, il gioco DICE potrebbe vedere giorni migliori. Parlando con *CNBC*, Pachter ha detto: «Anche se *Star Wars Battlefront II* ha avuto un debutto più debole del previsto in termini di vendite, crediamo che la lealtà dei fan di *Star Wars*, il fascino del gioco come regalo natalizio e l'uscita di *Star Wars : The Last Jedi* il 15 dicembre, possano avere effetto positivo sulle vendite del gioco». Resta da vedere se le previsioni di Pachter si dimostreranno affidabili. *Star Wars Battlefront II* è ora disponibile per PC, PlayStation 4 e Xbox One.

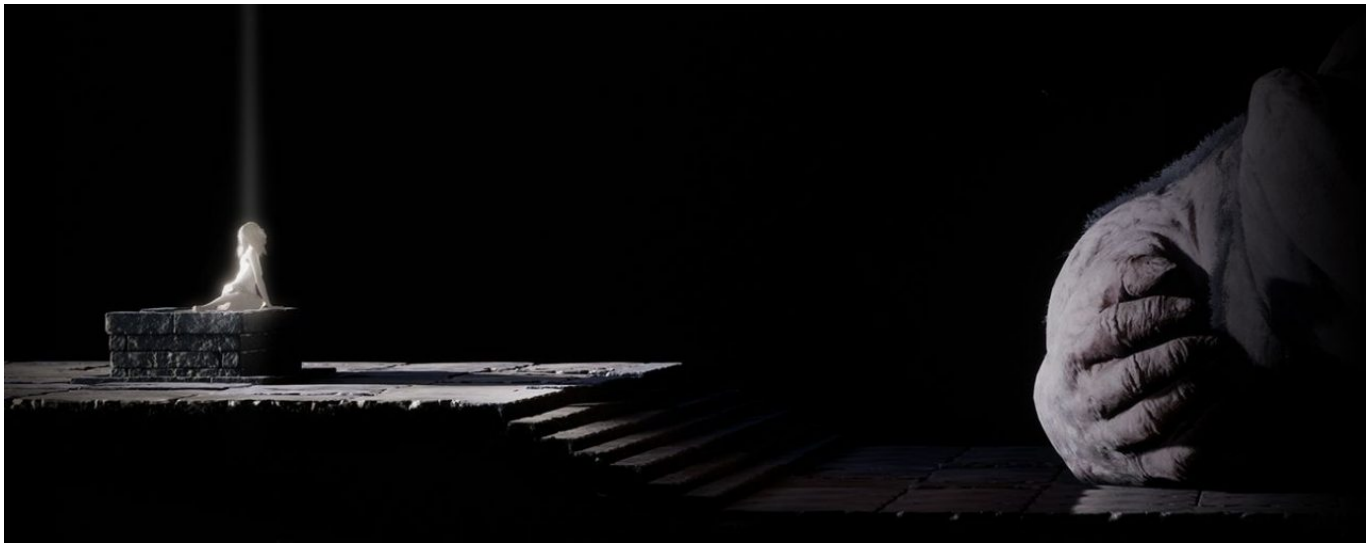
Il remake di Secret of Mana valutato dal PEGI americano

La **ERSB**, equivalente nordamericano del **PEGI** europeo, ha recentemente valutato il remake di ***Secret of Mana*** con il rating di E10+, ovvero **dai dieci anni in su**.
Al contrario della versione mobile e quella uscita su **Nintendo Wii**, la commissione ha deciso di dare tale rating a causa di "alcuni doppi sensi" e un "moderato numero di scollature".

Secret of Mana è un *JRPG* a tinte fantasy uscito originariamente per **Super Nintendo** nel 1993 e sviluppato da **Square Enix**. La sua particolarità era quella di offrire un *co-op* locale fino a tre giocatori.
Il remake è in uscita per il 15 febbraio 2018 per **PC**, **Playstation Vita** e per **Playstation 4**, con quest'ultima che beneficerà anche di una versione fisica acquistabile nei rivenditori specializzati.

Indizi sul nuovo titolo di Fumito Ueda

Fumito Ueda, direttore di ***The Last Guardian***, molto prima dell'annuncio del gioco, aveva postato un'immagine che mostrava le catene di Trico, piume e zanne. Sul sito web ufficiale di **genDesign,** studio fondato dal game director giapponese, è comparsa una concept art di quello che potrebbe essere il nuovo titolo in lavorazione.
Il disegno mostra una colomba in volo sopra una ragazza seduta in cima a una scalinata su cui cade perpendicolare un raggio di luce bianca. Sulla destra, si vede un grande pugno chiuso di quello che è presumibilmente un gigantesco personaggio, caratteristica che pare ormai una costante dei titoli di Fumito Ueda.



Il prossimo Nintendo Direct sarà l'11 gennaio?

Ora che il 2017 è finito, tiriamo le somme: **Switch** ha superato ogni aspettativa in fatto di vendite con oltre 10 milioni di copie vendute in 10 mesi, e offrendo già una discreta gamma di titoli, tra esclusive, indie, porting e multipiattaforma. Il futuro della console ibrida, almeno per quest anno, potrebbe rimanere altrettanto florido grazie a una lista di 8 nuovi giochi che, non ancora

ufficialmente annunciati, sembrano essere usciti allo scoperto grazie ad **Amazon**, avendo già reso disponibili i preordini dei suddetti (visibili cliccando qui), oltre ad alcuni accessori. Un particolare placeholder indica chiaramente che uno dei titoli in questione (chiamato *Project Octopath Traveler*) sia «appena stato annunciato a un evento», evento che però **Nintendo** non ha ancora confermato, ma di cui si specula da tempo, arrivando addirittura a un'ipotetica data: **11 gennaio 2018**. Se così fosse, non si dovrà aspettare molto per avere la conferma da parte della grande N, o la negazione, del leak di Amazon.

PUBG: Bluehole parla di un ipotetica versione PS4

Chang Han Kim, **CEO** di ***PUBG Corporation***, in seguito ad un intervista, è tornato a discutere dei progetti ambiziosi che la compagnia ha attualmente in mente per il suo titolo. In particolare gli è stato chiesto se il gioco, attualmente disponibile su PC e Xbox One, avrà una versione tutta sua anche su **PlayStation 4**.

Questa la risposta del **CEO**:

> **"Dal momento che sarà un titolo esclusivo per Xbox One per il momento, ci concentreremo sul completare l'attuale versione del gioco. Se si presenterà l'opportunità, il nostro obiettivo finale sarà quello di lanciare il titolo su ogni piattaforma."**

Sembra confermata dunque l'esclusività temporanea detenuta da **Microsoft** su console e la volontà di **Bluehole** di portare il gioco prima o poi anche su **Ps4** e, perchè no, su **Nintendo Switch**.

Si è poi discusso di un'ipotetica estensione di *PlayerUnknow's Battlegrounds* ad altri media, oltre quello videoludico.

> **"Il mio sogno è che PUBG possa diventare un franchise multimediale, vogliamo entrare a far parte di diversi tipi di industrie oltre a quella videoludica, come ad esempio gli eSport, il cinema, i cartoni animati, film d'animazione ecc. A dirla tutta abbiamo già ricevuto telefonate da Hollywood e Netflix."**