Dead Space gratis su Origin per un tempo limitato

Dead Space per **PC Windows** è attualmente disponibile gratuitamente tramite il servizio **Origin** di **EA** come parte del programma dell'azienda "**Offre la ditta**". Il gioco è **completo al 100%** per un periodo limitato, quindi assicuratevi di prenderlo prima che la promozione scada. *Dead Space* è stato rilasciato nel 2008, quindi non necessita di un PC di ultima generazione per poter godere al meglio l'esperienza di gioco, ma rimane comunque uno dei migliori titoli horror pubblicati negli ultimi dieci anni.

Amnesia: Collection gratis su Humble Bundle

Il noto store di key **Humble Bundle** ha reso disponibile per 48 ore ***Amnesia: Collection*****,** gratuitamente. La *Collection* in questione è valida per la versione PC nonostante esclusiva PS4, e suddivisa in due parti, ***Amnesia: The Dark Descent*** e ***Amnesia: A Machine for Pigs*****.** Questi due giochi sono enormemente consigliati per gli amanti dell'horror e vi terranno incollati allo schermo per ore.

Rumor: Microsoft lavora a nuovo controller Elite

Il controller **Xbox Elite** di **Microsoft** è costoso, ma probabilmente è la scelta ideale per i possessori di **Xbox One** che desiderano un gamepad adatto alle proprie esigenze. E a quanto pare, c'è abbastanza richiesta per meritare un seguito. **Molti *rumor*** sembrano indicare l'arrivo di un nuovo controller **Elite** che si basa sulle esperienze apprese dal primo modello. Se i suggerimenti sono accurati, include **Bluetooth** (per collegarsi senza problemi al PC), una connessione cablata **USB-C**, un connettore di ricarica **Apple MagSafe** sul retro e una **batteria incorporata**. E naturalmente, più modifiche per i giocatori che desiderano controlli più precisi e personalizzati.

Stando a queste informazioni, che – come riportato in basso – sono contornate di immagini del nuovo controller (dall'utente **Reddit EDDS86**), il nuovo dispositivo avrebbe nuovi *grip* in modo da assicurare che le proprie mani siano ben salde durante sessioni frenetiche, un interruttore a tre profili, tre livelli di blocco per il *trigger,* e la regolazione della tensione degli *stick*. Dato che Microsoft fece domanda per un brevetto su quest'ultimi a dicembre, pare che tali affermazioni siano veritiere. Tra l'altro, una fonte di **The Verge**, confermerebbe tutto.
Non si fa menzione alla data di rilascio del controller sul mercato ma Microsoft, abitualmente, tende

a riservare i suoi grandi annunci per l'**E3** (quest'anno, a metà giugno), rilasciando tutte le informazioni del caso.

NVIDIA: nuovi driver e funzionalità

NVIDIA ha rilasciato un nuovo driver **GeForce** (versione **390.65, WHQL**) che include una patch di sicurezza per la vulnerabilità di ***Spectre***. Inoltre, questo nuovo driver fornisce ottimizzazioni per ***Fortnite***, aggiungendo il supporto a ***ShadowPlay Highlights***, nella sua modalità **Battle Royale**, come, del resto, ***ELEX*** e ***Crossout***. Ultimo, ma non meno importante, il driver GeForce 390.65 aggiunge il supporto per la versione beta di **NVIDIA *Freestyle*,** che consentirà ai giocatori di applicare filtri di post-elaborazione ai propri giochi; già dall'*overlay* in-game, si potrà modificare aspetto ed effetti agendo sulla saturazione dei colori. Al lancio ci saranno un totale di **15 filtri** con 38 diverse impostazioni:

- **Color**
- **Colorblind**
- **Contrast**
- **Details**
- **Exposure**
- **Half Tone**
- **Mood**
- **Night Mode**
- **Retro**
- **Sepia**
- **Vignette**
- **Depth of Field**
- **Special FX**
- **Adjustments**

Freestyle consentirà di essere creativi con i propri giochi: si potrà, per esempio, creare un filtro a tema pre-bellico retrò per il proprio FPS preferito o migliorare il colore e il contrasto per rendere il gioco più fotorealistico. Un uso più approfondito del programma permetterà una modalità adatta a chi soffre di daltonismo e persino una modalità notturna, riducendo la luce blu proiettata dallo schermo, in modo che gli utenti possano dormire meglio dopo una notte di gioco. *Freestyle* è stato integrato a livello di driver per fornire "compatibilità perfetta". Per più info ecco i ***changelog*** e il **link** dove scaricare i driver selezionando il vostro sistema operativo e la propria GPU.

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 !

Ubisoft anticipa i regali di Natale con ben 3 giochi gratuiti

Da poche ore l'editore francese **Ubisoft** ha aperto gli **Happy Playdays**, un'iniziativa dove vengono messi a disposizione ben 3 giochi gratuiti per PC sullo store di Ubisoft, **uPlay**. I giochi in questione sono: ***Watch Dogs***, ***World in Conflict: Complete Edition*** e ***Assassin's Creed IV Black Flag***. Ubisoft si veste da Babbo Natale per anticipare i regali di natale, ma il tempo a disposizione è limitato fino al **23 Dicembre**.

NVIDIA: presentata TITAN V Volta, un mostro di potenza da 3000$

NVIDIA ha appena **annunciato** la sua ultima scheda grafica **TITAN** basata sull'architettura **Volta**, la **TITAN V**. NVIDIA TITAN V presenta le più recenti tecnologie GPU come l'architettura Volta **12nm** accoppiata con **12 GB** di memoria **HBM2**.

NVIDIA TITAN V, uno mostro da 3000$ con 5120 CUDA Cores, 12 GB HBM2 VRAM e tecnologia a 12nm

La scheda grafica NVIDIA TITAN V è dotata dell'ultima architettura Volta da 12nm e, come tale, è dotata delle più recenti tecnologie che NVIDIA ha da offrire. In primo piano nella famiglia TITAN, la GPU mirerà al mercato dei prosumer e in quanto tale, ci si può aspettare un prezzo molto alto in quanto questa bestia avrà un costo di **3000$**. Annunciata dal fondatore e CEO di NVIDIA **Jensen Huang** alla conferenza annuale **NIPS**, TITAN V eccelle nell'elaborazione computazionale per la simulazione scientifica. I suoi **21,1 miliardi di transistor** erogano **110 teraflops** di potenza, **9 volte** quella del suo predecessore, con un'estrema efficienza energetica.

> **«La nostra visione di Volta era quella di spingere i limiti estremi del calcolo ad alte prestazioni e dell'intelligenza artificiale. Abbiamo aperto nuovi orizzonti con la nuova architettura del processore a 12 nm, le istruzioni, i formati numerici, l'architettura della memoria e i collegamenti del processore. Con TITAN V, stiamo mettendo Volta nelle mani di ricercatori e scienziati di tutto il mondo. Non vedo l'ora di vedere le loro scoperte rivoluzionarie»**
> **(Jensen Huang, CEO di NVIDIA)**

Non si ottiene solo la straordinaria nuova architettura Volta "**GV100**", ma gli acquirenti hanno anche 12 GB di memoria HBM2. Questa è la prima scheda grafica TITAN e anche la prima linea di schede grafiche NVIDIA con memoria HBM2.

La NVIDIA TITAN V è basata sull'architettura GV100 e dispone di un totale di **5120 CUDA core** e **320 texture unit**. Questa è esattamente la stessa quantità di core presenti su **Tesla V100**. Oltre ai core regolari, la scheda include anche **640 Tensor Core** all'interno della GPU Volta. Questi sono orientati alla massima performance in quanto la scheda può generare fino a **110 TFLOPS** di prestazioni per algoritmi relativi all'IA. La totalità del core è sincronizzata su base **1200 MHz** e **boost a 1455 MHz**. Anche con caratteristiche così pesanti, la scheda richiede solo un connettore di alimentazione a 8 e 6 pin per l'avvio e arriva a consumare fino 250 W. Quindi, venendo alla VRAM HBM2, come detto ci sono 12 GB con una velocità dati di **1,7 Gbps** lungo un bus di memoria a **3072 bit**. Questo dà alla scheda una larghezza di banda totale di **652,8 GB/s**, che è molto più veloce della precedente **TITAN Xp**. Rispetto a Tesla V100, stiamo considerando un'interfaccia bus cut down (**4096-bit vs 3072-bit**) e anche una VRAM inferiore di **12 GB** rispetto a **16 GB** su quella scheda.

Nel complesso, questa scheda grafica può essere utilizzata per carichi di lavoro sia professionali che regolari come i giochi, e sarà interessante vedere come si comporterà questo asso di NVIDIA. Mentre il prezzo è decisamente alto, a bordo di TITAN V ci sono molte cose che le normali schede non hanno, elemento che la rende adatta a carichi di lavoro professionali. Queste funzionalità

includono:

- **Calculation Cores FP64 dedicati**
- **Tensor Calculation Cores dedicati**
- **12 GB HBM2 con Interfaccia a 3072-bit**
- **Interfaccia NVLINK 2.0**

Foto dettagliate della TITAN V

A parte le specifiche, NVIDIA TITAN V offre lo stesso **Cooler NVTTM**, che abbiamo imparato a conoscere e amare nelle schede della serie **Pascal GeForce 10**. La GPU presenta solo una differenza tra le altre della serie 1000: il nome inciso sulla scocca. Inoltre è dotata di un magnifico corpo in alluminio **pressofuso d'oro** e di un sistema di raffreddamento delle **head pipe** superiore per le migliori performance termiche possibili. Il **PCB è un DrMOS a 16 fasi** con funzionalità di monitoraggio della corrente e di monitoraggio termico in tempo reale.

Intel Core i3-8350K: grazie a una modifica è possibile usarlo su piattaforma z170

Un **Intel Core i3 8350K** è stato accoppiato a una scheda madre con chipset **z170**, una combinazione pensata non fattibile, ma un utente dalla Cina è riuscito nell'impresa intervenendo con qualche modifica.

La scheda madre utilizzata per questa mod non è sicuramente economica. Parliamo di una **z170A Xpower Titanium** di **MSI**, che probabilmente potrebbe supportare anche un **i7 8700K**, grazie alle fasi di cui dispone per un **overclock** spinto. Il modder è riuscito ad avviare correttamente il sistema operativo Windows con il processore i3 8350K installato sulla scheda madre z170. Modifiche del **BIOS** e modifiche al **microcode** erano necessarie per farlo funzionare. Tuttavia, dire che questa mod funzioni perfettamente sarebbe un'esagerazione. La **GPU** integrata non è infatti disponibile, e anche lo slot **PCI-Express** primario non funziona, ma quelli potrebbero essere solo problemi specifici della scheda madre/driver. Ulteriori modifiche potrebbero probabilmente risolvere tali problemi. **Intel** afferma che le modifiche di erogazione dell'alimentazione per la **+12 V** di **Coffee Lake-S LGA1151** rendevano impossibile la compatibilità con le versioni precedenti. Tuttavia, poche settimane fa **Andrew Wu** di **ASUS** ha confermato che la decisione di disabilitare il supporto **CFL-S** per z170 / z270 è stata dettata da Intel, mentre le schede madri più vecchie potevano facilmente supportarle.

Intel: 9a generazione con più core per competere contro Ryzen 2

Sulla base di recenti **rumor** da parte di **VideoCardz** riguardo **Intel**, fonti cinesi stanno riportando informazioni attraverso le dati acquisiti dai produttori di schede madri di Taiwan riguardo la nuova generazione di punta di Intel (9a generazione), la quale comprenderà più core rispetto all'attuale processore mainstream più veloce.

Intel Core i7-9700K con 8 core e 16 thread, Intel Core i5 e i3 ancora più potenti

Non c'era alcun dubbio che i processori mainstream della 9a generazione di Intel non avrebbero ricevuto alcun **aumento dei core** entro il prossimo anno. Sono trapelate alcune diapositive e l'anno prossimo Intel avrà abbastanza tempo per modificare il proprio processo produttivo e la progettazione dell'architettura per ospitare più core. Tra gli **HKEPC**, che sono stati in grado di ottenere informazioni dai produttori di schede madri di **Taiwan**, si è diffusa la voce che l'ammiraglia di 9a generazione che sarà conosciuta come **Intel Core i7-9700K**, comprenderà **8 core e 16 thread**. Non si parla di quale tecnologia di processo verranno utilizzate dai nuovi processori, ma si crede che sia una versione aggiornata dell'attuale processo **14nm ++**. C'è anche un rumor interessante per quanto riguarda i processori **Core i5** e **Core i3**. Secondo la stessa fonte, i chip Core i5 di prossima generazione di Intel saranno dotati di una CPU a **6 core e 12 thread**. Attualmente, tutti i chip della serie Intel Core i5 sono dotati di **6 core e 6 thread** mentre la linea i7 presenta **6 core e 12 thread**. La serie Core i3 d'altra parte otterrà anche il supporto **multi-threading**, il che significa che avremo un **4 core e 8 thread** e non più il **4 core e 4 thread** che siamo abituati a vedere al momento sui chip i3 di **Coffee Lake**.

Specifiche della 9a generazione di Intel contro l'attuale generazione

La nuova generazione di Intel si scontrerà contro i Ryzen 2 di AMD

È facile dire che Coffee Lake è stata una risposta immediata e affrettata a **Ryzen** di **AMD**, ma con la 9a generazione Intel avrà una buona quantità di tempo per rilasciare un forte concorrente. La nuova generazione di AMD, **Ryzen 2**, dovrebbe debuttare il prossimo anno e utilizzerà delle CPU **Zen** ottimizzate per una maggiore leva prestazionale e una maggiore efficienza. Al momento non si parla di un aumento di core, ma AMD potrebbe intraprendere questa strada da quando le guerre dei core tra Intel e AMD sono in aumento sia nei segmenti mainstream che in quelli **HEDT**. La famiglia Intel di 9a generazione sarà supportata sulla piattaforma **z390** o serie **300**, mentre AMD dovrebbe lanciare una linea di aggiornamento delle schede madri, ma manterrà anche la compatibilità per la nuova famiglia di CPU su schede madri esistenti.

Specifiche dei PCH riguardo Kaby Lake Refresh e Cannon Lake

La linea di **Ryzen 7** si scontrerà contro il Core i7, **Ryzen 5** andrà contro il Core i5 nel segmento di budget, ed è qua che si svolgerà la vera battaglia. Nel segmento entry level e il segmento value vediamo invece i chip Core i3 e **Ryzen 3** che punteranno al mercato statunitense a partire dai **200**

$. Sarà una competizione interessante quella dell'anno prossimo nel segmento **desktop** e **laptop** in cui AMD sta risorgento dopo anni di silenzio.

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».