Bitdefender

Intel: nuova impattante vulnerabilità scoperta dai ricercatori Bitdefender, consente il furto di dati sensibili e nessuna soluzione può risolverla

Riguarda tutte le moderne CPU Intel nei server (prodotti tra il 2012 e il 2020), nei desktop e nei laptop, compresa la nona generazione di CPU ed è particolarmente impattante negli ambienti multi-tenant, come workstation aziendali o server dei data center

Load Value Injection (CVE-2020-0551)

Milano, 11 Marzo 2020 – Bitdefender rende nota una nuova impattante vulnerabilità scoperta dai propri ricercatori e che riguarda tutte le moderne CPU Intel nei server (prodotti tra il 2012 e il 2020), nei desktop e nei laptop, compresa la nona generazione di CPU Intel. Questa vulnerabilità può portare alla fuga di informazioni in determinati scenari, è particolarmente impattante negli ambienti multi-tenant, come workstation aziendali o server dei data center e al momento nessuna soluzione è in grado di risolverla.

In dettaglio questa nuova vulnerabillità consente all'aggressore di iniettare valori anomali in determinate strutture di microarchitettura che vengono poi utilizzati dalla vittima, che potrebbe portare ad una fuoriuscita di informazioni riservate.

Rischi

Questa vulnerabilità, permette a un aggressore di influenzare le funzionalità a livello hardware di Intel per far trapelare i dati. Può consentire a un malintenzionato che ha accesso a un'infrastruttura condivisa (come i fornitori di cloud pubblici o altri ambienti condivisi dell'impresa) di divulgare dati a cui altrimenti non avrebbe accesso. Questo tipo di attacco può teoricamente funzionare oltre tutti i confini della sicurezza: da processo a processo, da modalità utente a modalità kernel, da modalità guest-mode a modalità root.

Questo tipo di attacco, come sopracitato, è particolarmente impattante negli ambienti multi-tenant, come workstation aziendali o server dei data center, dove un utente con meno privilegi potrebbe far trapelare informazioni sensibili provenienti da un utente con più privilegi o da un differente ambiente virtualizzato bypassando l'hypervisor.

Il rischio più ovvio è il furto di dati, poiché un aggressore con meno privilegi può campionare informazioni che dovrebbero essere tenute private dalle misure di sicurezza a livello di chip o di microcodice. Queste informazioni possono essere di qualsiasi tipo, dai dati relativi alle interferenze nel sistema operativo alle chiavi di crittografia o alle password in memoria. Nel peggiore dei casi un aggressore potrebbe godere di un controllo significativo del server (o dell'endpoint) vulnerabile e dei dati memorizzati su di esso.

Impatto

Si stima che Intel alimenti il 90% dei server in produzione fino ad oggi.

Misure Correttive

Le misure correttive esistenti per **Meltdown, Spectre e MDS non sono sufficienti**. Per rimuovere **completamente** la nuova vulnerabilità si devono **disabilitare le funzionalità** che forniscono elevate **prestazioni**, come l'Hyper-threading, o **sostituire l'hardware.**
Inoltre, occorre assicurarsi di aver applicato le **ultime patch di microcodice della CPU** e di aver **aggiornato** il **sistema operativo**.

Allo stesso modo, la creazione di meccanismi di mitigazione può essere **molto complessa** e **compromettere le prestazioni**.
Per esempio, "La tecnologia Hyper-Threading consente performance superiori del 30% nei benchmark di applicazioni server più comuni per questa tecnologia" https://software.intel.com/en-us/articles/how-to-determine-the-effectiveness-of-hyper-threading-technology-with-an-application

Bitdefender raccomanda qui di seguito le **3 azioni più urgenti** che devono essere intraprese dal reparto IT di **qualsiasi azienda** che utilizza questi processori:

1. Installare le patch (microcodice, sistema operativo, hypervisor) non appena sono disponibili.
2. Installare una soluzione di sicurezza che fornisca visibilità e contesto a livello di hypervisor.
3. Verificare i sistemi critici per identificare eventuali segni di intrusione, se possibile.

Bitdefender ha avvertito Intel di questo attacco il 10 febbraio prima della divulgazione pubblica, anche se non è stato il primo a segnalarlo*. Il 25 febbraio, Intel ha riconosciuto questa vulnerabilità. Le ricerche di Bitdefender sono accreditate da un sintetico Proof of Concept.

Per ulteriori approfondimenti:

- Whitepaper:
- Sito Internet
- Blogpost su Business Insight

***Ringraziamenti** Bitdefender desidera ringraziare per la loro collaborazione i ricercatori che per primi hanno segnalato questo problema a Intel : Jo Van Bulck, Daniel Moghimi, Michael Schwarz, Moritz Lipp, Marina Minkin, Daniel Genkin, Yuval Yarom, Berk Sunar, Daniel Gruss, and Frank Piessens.

A proposito di Bitdefender

Bitdefender è un leader globale della sicurezza informatica che protegge oltre 500 milioni di sistemi in più di 150 paesi. Dal 2001, l'innovazione di Bitdefender ha costantemente fornito prodotti di sicurezza pluripremiati e informazioni sulle minacce per la casa connessa in modo intelligente, gli utenti mobili, le aziende moderne e le loro reti, dispositivi, data center e infrastrutture cloud. Oggi, Bitdefender e i suoi Labs sono anche il fornitore di fiducia, integrato in oltre il 38% delle soluzioni di sicurezza del mondo. Riconosciuta dall'industria, rispettata dai fornitori ed evangelizzata dai clienti, Bitdefender è la società di sicurezza informatica di cui puoi fidarti e su cui puoi fare affidamento.

***

Per ulteriori informazioni
Prima Pagina Comunicazione
02/91339820
Tania Acerbi, Monica Fecchio, Elisa Pagano
tania@primapagina.it
monica@primapagina.it
elisa@primapagina.it