Hewlett Packard Enterprise

Report

Guida per i clienti HPE. Mitigazione della vulnerabilità dei microprocessori rilevata nell'intero settore

Ultimo aggiornamento: 21 marzo 2018

Contents

Sono finalmente disponibili tutte le ROM per sistemi server HPE Gen10, Gen9, Gen8, G7 e G6 basati su Intel

Il 19 marzo 2018, le nuove ROM di sistema per tutti i server HPE Gen10, Gen9, Gen8, G7 e G6 basati su Intel® sono state pubblicate sul sito Web del supporto HPE. HPE consiglia ai clienti di aggiornare i server HPE alle nuove ROM di sistema, per contenere il rischio associato alle vulnerabilità di analisi del canale collaterale.

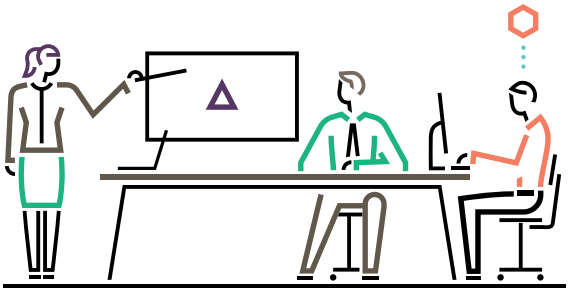
In aggiunta, la ROM di sistema per il server HPE ProLiant DL385 Gen10 basato su AMD, che include il supporto per il contenimento della vulnerabilità di analisi del canale collaterale, è disponibile nel sito Web del supporto HPE già dal mese di gennaio 2018.

Avviso Intel: 22 gennaio 2018

Abbiamo informato i clienti che, il 22 gennaio 2018, Intel ha pubblicato una dichiarazione relativa ai problemi associati alla patch di microcodice Intel con lo scopo di rimuovere la vulnerabilità di analisi del canale collaterale (Side-Channel Analysis). Ai clienti HPE che hanno scaricato una ROM di sistema specifica di questa vulnerabilità, per un server basato su Intel, fra il 5 gennaio 2018 e il 21 gennaio 2018, HPE consiglia di scaricare le nuove ROM di sistema attualmente disponibili e utilizzarle per aggiornare i server.

Per ulteriori informazioni, visita il sito Intel Security Exploit Newsroom and HPE Customer Advisory.

Situazione generale



Nelle moderne architetture di microprocessore è stata recentemente individuata una vulnerabilità che interessa l'intero settore. Secondo i nuovi studi sulla sicurezza, esistono sistemi di analisi software che, se utilizzati da un malintenzionato, permettono di raccogliere illegalmente dati sensibili da dispositivi informatici correttamente funzionanti. Spesso indicato come "metodo di analisi del canale collaterale", Spectre o Meltdown, questo problema interessa le architetture di microprocessore di vari fornitori di CPU, tra cui Intel, AMD e Arm®.

I fornitori di hardware e software di tutto il settore, compresa HPE, stanno collaborando per rendere disponibili soluzioni appropriate a questo problema. Questo documento HPE è una guida per i clienti, con lo scopo di semplificare le misure di contenimento dei rischi correlati a tale vulnerabilità.
Include istruzioni dettagliate e un elenco di collegamenti importanti per accedere agli aggiornamenti dei sistemi operativi più comuni e dei microcodici utilizzati nelle attuali generazioni di server HPE. HPE consiglia inoltre ai propri clienti di consultare le informazioni pubblicate dai fornitori di microprocessori, ovvero Intel, AMD e Arm.

Indicazioni per i clienti HPE

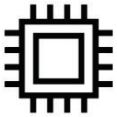
La sicurezza dei prodotti HPE ha la massima priorità e continuiamo a collaborare in modo proattivo con fornitori di sistemi operativi e microprocessori per sviluppare aggiornamenti software e firmware in grado di ridurre l'impatto della vulnerabilità.

Un aspetto importante del metodo di analisi del canale collaterale è costituito dal fatto che richiede malware in esecuzione sul sistema locale. Questa particolare vulnerabilità non consente processi diretti di alterazione, eliminazione, distruzione o crittografia dei dati, che potrebbero essere tuttavia estratti dai sistemi informatici. Di conseguenza, è importante rispettare le procedure di sicurezza corrette, che comprendono l'aggiornamento costante di software e firmware. Il rispetto delle best practice di sicurezza e la distribuzione dei server HPE Gen10 con la tecnologia sicura Silicon Root of Trust contribuisce a proteggere l'azienda dagli attacchi dannosi.

Procedura di contenimento consigliata

HPE consiglia a tutti i clienti di seguire questa procedura per i prodotti server e di storage, al fine di determinare il livello di rischio e definire un piano di contenimento.

Per i prodotti server:

1	2	3	4
			
Verifica se possiedi un sistema soggetto a questa vulnerabilità. Puoi consultare l'elenco aggiornato dei prodotti interessati nella **pagina Web di HPE dedicata alle vulnerabilità**.	Se il tuo sistema è coinvolto, scarica e installa l'aggiornamento del sistema operativo distribuito dal relativo fornitore. Troverai le istruzioni sulle opportune misure da adottare in funzione del sistema utilizzato nel **Bollettino sulla sicurezza HPE**.*	Aggiorna la ROM di sistema a una revisione contenente un microcodice aggiornato fornito da HPE, quando disponibile. Troverai le istruzioni sulle opportune misure da adottare in funzione del sistema utilizzato nel **Bollettino sulla sicurezza HPE**.**	Riavvia il sistema come richiesto, per garantire l'implementazione completa dei nuovi aggiornamenti.

* L'applicazione degli aggiornamenti del sistema operativo fornisce protezione da alcune varianti della vulnerabilità, anche se gli aggiornamenti della ROM di sistema non sono disponibili.

** Ai clienti HPE che hanno scaricato una ROM di sistema specifica di questa vulnerabilità, per un server basato su Intel, fra il 5 gennaio 2018 e il 21 gennaio 2018, HPE consiglia di scaricare le nuove ROM di sistema attualmente disponibili e utilizzarle per aggiornare i server.

Per i prodotti di storage:

1	2
	
Verifica se possiedi un sistema soggetto a questa vulnerabilità. Puoi consultare l'elenco aggiornato dei prodotti interessati nella **pagina Web di HPE dedicata alle vulnerabilità.**	Se il tuo sistema è coinvolto e quindi considerato vulnerabile, utilizza il collegamento alle istruzioni di **mitigazione** disponibile nella **pagina Web di HPE dedicata alle vulnerabilità.**

Domande frequenti

1. La vulnerabilità dei microprocessori riguarda tutti i fornitori del settore tecnologico o soltanto HPE?

La vulnerabilità dei microprocessori interessa tutti i fornitori di tecnologia che utilizzano i moderni microprocessori e non è specifica di HPE. Tutti i prodotti e le soluzioni interessati dalla vulnerabilità richiedono gli aggiornamenti appropriati del sistema operativo e della ROM. Intel ha dichiarato che i processori Itanium® non sono affetti dalla vulnerabilità di analisi del canale collaterale.

2. Quali sono i prodotti e le soluzioni HPE interessati?

Tutti i prodotti HPE che includono i microprocessori interessati sono potenzialmente vulnerabili. Per identificare i prodotti e le soluzioni HPE interessati dal problema, visita il sito Web di HPE dedicato alle vulnerabilità. HPE provvederà ad aggiornare l'elenco dei sistemi come necessario.

3. La vulnerabilità dei microprocessori è dovuta a un attacco o a una violazione in atto?

No, non ci sono stati attacchi noti. La vulnerabilità è causata da un difetto di progettazione che, se analizzato tramite la metodologia del canale collaterale, può consentire ai malintenzionati di accedere ai dati. L'applicazione degli aggiornamenti appropriati del sistema operativo e del microprocessore per i sistemi HPE permette di contenere il rischio associato alla vulnerabilità.

4. Qual è la portata della vulnerabilità di sicurezza?

Gli ultimi studi sulla sicurezza hanno permesso di individuare metodi di analisi del software che, se utilizzati da malintenzionati, consentono di raccogliere illegalmente dati sensibili da dispositivi informatici correttamente funzionanti. Per ulteriori informazioni, puoi fare riferimento alle seguenti CVE: CVE-2017-5715, CVE-2017-5753, CVE-2017-5754.

5. Qual è la soluzione?

Per risolvere il problema sono necessari sia un aggiornamento del sistema operativo, messo a disposizione dal relativo fornitore, sia un aggiornamento della ROM di sistema, fornito da HPE. A seconda dei sistemi HPE utilizzati, puoi trovare le istruzioni sulle misure appropriate nel
sito Web di HPE dedicato alle vulnerabilità.

Se sei un cliente HPE Pointnext e ritieni che il tuo sistema sia interessato dal problema, contatta il responsabile dell'assistenza.

Se sei un cliente HPE Storage, puoi trovare le istruzioni sulle misure appropriate nel sito Web di HPE dedicato alle vulnerabilità. Le procedure di risoluzione per i prodotti di storage HPE possono essere diverse dai rimedi per i prodotti server HPE. Per informazioni dettagliate sullo storage, visita il sito Web di HPE dedicato alle vulnerabilità. Per i prodotti software come StoreVirtual VSA, StoreOnce VSA, RMC e altri titoli eseguibili sui server x86, è consigliabile fare riferimento alle comunicazioni del fornitore del server x86.

6. Per scaricare e installare gli aggiornamenti HPE per la ROM di sistema è obbligatorio disporre di un contratto attivo o di una garanzia?

No. Per gli aggiornamenti HPE della ROM di sistema destinati ai prodotti e alle soluzioni interessati dalla vulnerabilità, se disponibili, non viene eseguito alcun controllo di idoneità.

7. Quali sono i sistemi operativi interessati?

Sono interessati i sistemi operativi Windows®, Linux® e VMware®. I fornitori dei sistemi operativi stanno pubblicando i necessari aggiornamenti delle patch. In base alla comunicazione attuale di Intel, i processori Itanium non sono interessati, pertanto i sistemi HP-UX, OpenVMS e i sistemi NonStop serie J e serie H con NonStop OS non risentono di questo problema. I sistemi NonStop serie L con NonStop OS sono invece interessati perché utilizzano processori x86. Sono interessati anche i componenti CLIM e NSC dei sistemi NonStop dotati di processori x86 e sistema operativo Linux o Windows. Per ulteriori informazioni, HPE consiglia di contattare i fornitori dei sistemi operativi, ovvero Microsoft®, VMware, SUSE e Red Hat®.

8. Quali sono i microprocessori interessati?

La maggior parte dei microprocessori con architetture moderne può essere soggetta al metodo di analisi del canale collaterale. Intel e AMD hanno informato HPE di propria iniziativa e stanno collaborando attivamente per fornire le soluzioni necessarie. Intel ha dichiarato che i processori Itanium non sono affetti dalla vulnerabilità di analisi del canale collaterale. Contatta gli altri fornitori di microprocessori per ricevere ulteriori informazioni.

9. Sono coinvolti anche altri produttori di hardware?

Sono potenzialmente vulnerabili tutti i produttori di hardware e i provider di servizi di cloud pubblico che usano le moderne architetture di microprocessore interessate. Possono essere coinvolti anche i telefoni cellulari e i computer client. Per maggiori dettagli, rivolgiti ai fornitori di questi prodotti.

10. Dopo l'applicazione delle patch sui miei sistemi, ci saranno effetti sulle prestazioni?

Nella maggior parte dei casi, è in genere prevedibile un impatto minimo sulle prestazioni, che varia in base al sistema operativo e al carico di lavoro. HPE e i suoi partner che si occupano di sistemi operativi e microprocessori continueranno a monitorare e caratterizzare i potenziali effetti sulle prestazioni nel tempo e forniranno ulteriori indicazioni a mano a mano che saranno disponibili nuovi dati.

11. Che ripercussioni avrà questa vulnerabilità dei microprocessori sui server HPE ProLiant e HPE Synergy Gen10, i server standard di settore più sicuri al mondo?[1]

La vulnerabilità dei microprocessori è un difetto dei moderni microprocessori, ma non sono stati rilevati attacchi noti associati a tale vulnerabilità. I server HPE Gen10 sono dotati dell'unica tecnologia Silicon Root of Trust originale. Questi circuiti personalizzati HPE assicurano una protezione senza precedenti dagli attacchi al firmware. Nonostante queste avanzate funzionalità di protezione, i clienti devono comunque applicare tutti gli aggiornamenti consigliati e seguire le best practice di sicurezza in relazione a questa particolare vulnerabilità.

12. Quali saranno le ripercussioni di questa vulnerabilità dei microprocessori per i clienti che valutano l'acquisto di prodotti HPE?

Possiamo garantire che le soluzioni di elaborazione HPE sono all'avanguardia in termini di sicurezza e qualità. La scoperta di questo difetto nei microprocessori, che riguarda l'intero settore, non dovrebbe influire in alcun modo sulle decisioni di acquisto delle soluzioni HPE. HPE continuerà a collaborare con Intel, AMD e Arm, assicurandosi che le soluzioni necessarie per i microprocessori impiegati nei nostri prodotti rimangano una priorità assoluta. Inoltre, l'applicazione degli aggiornamenti ai microprocessori, unita all'adozione della tecnologia Silicon Root of Trust di HPE presente solo nei server HPE Gen10, garantisce piattaforme di elaborazione conformi ai massimi standard di sicurezza del settore.

13. HPE fornirà altri aggiornamenti relativi a questa vulnerabilità?

Sì, HPE continuerà a pubblicare aggiornamenti non appena saranno disponibili ulteriori informazioni e dettagli. Visita il sito Web di HPE dedicato alle vulnerabilità.

14. HPE ha recentemente rilasciato gli aggiornamenti della ROM di sistema per i prodotti server HPE ProLiant, HPE Synergy, HPE Superdome Flex e HPE Superdome X. Perché non riesco a trovarli?

A partire dal 19 marzo 2018 gli aggiornamenti sono disponibili per tutti i server HPE Gen10, Gen9, Gen8, G7 e G6 basati su Intel e per il server HPE ProLiant DL385 Gen10 basato su AMD.

Il 22 gennaio 2018, Intel ha pubblicato una dichiarazione relativa ai problemi associati alla patch di microcodice Intel rilasciata al fine di rimuovere la vulnerabilità di analisi del canale collaterale (Side-Channel Analysis). In tale occasione Intel ha consigliato ai clienti di interrompere la distribuzione delle ROM di sistema che includono questa patch di microcodice e ripristinare la versione precedente della ROM, per evitare comportamenti imprevisti del sistema. Di conseguenza, gli aggiornamenti della ROM di sistema per i prodotti server HPE ProLiant, HPE Synergy, HPE Superdome Flex e HPE Superdome X sono stati rimossi dal sito del supporto HPE.

Dopo tale data, Intel ha effettuato varie revisioni del microcodice e le ROM di sistema aggiornate ora sono disponibili per tutti i server HPE Gen10, Gen9, Gen8, G7 e G6 basati su Intel. Le revisioni aggiornate delle ROM di sistema per le altre piattaforme verranno rilasciate da HPE dopo che Intel avrà fornito i microcodici aggiornati.

[1] Sulla base dei risultati dei test di penetrazione della sicurezza informatica condotti da un'azienda esterna su una serie di prodotti server di diversi fornitori nel maggio 2017.

15. Quali generazioni di server HPE riceveranno gli aggiornamenti delle ROM di sistema che includono i microcodici per il contenimento della vulnerabilità di analisi del canale collaterale?

HPE lavora a stretto contatto con i fornitori di microprocessori allo scopo di fornire gli aggiornamenti delle ROM di sistema per i server HPE di generazione Gen10, Gen9, Gen8, G7 e precedenti, a mano a mano che gli aggiornamenti di microcodici vengono resi disponibili dai fornitori dei processori.

Per ulteriori informazioni, domande o richieste di assistenza, contatta direttamente il tuo rappresentante commerciale o partner autorizzato HPE.

Registrati per ricevere gli aggiornamenti

a00039576ENW, marzo 2018, Rev. 2