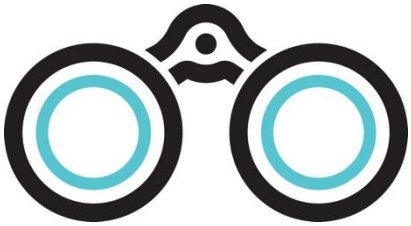
Hewlett Packard Enterprise

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

5 gennaio 2018

Premesse



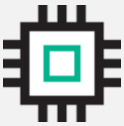
È stata recentemente individuata una vulnerabilità nelle moderne architetture dei microprocessori che interessa l'intero settore. Secondo nuovi studi sulla sicurezza, esistono sistemi di analisi software che, se utilizzati da malintenzionati, possono raccogliere illecitamente dati sensibili da dispositivi informatici correttamente funzionanti. Spesso indicata come "metodo di analisi side-channel", Spectre o Meltdown, questa falla riguarda architetture di microprocessori di diversi fornitori di CPU, tra cui Intel, AMD e ARM.

I fornitori di hardware e software dell'intero settore, compresa HPE, stanno lavorando congiuntamente per rendere disponibili le opportune soluzioni. Il presente documento HPE rappresenta una guida per i clienti intesa a semplificare le attività di riduzione dei rischi correlati a tale vulnerabilità; include istruzioni dettagliate e un elenco di link importanti per accedere agli aggiornamenti dei più comuni sistemi operativi e microcodici utilizzati nelle attuali generazioni di server HPE. HPE consiglia inoltre ai propri clienti di consultare le informazioni pubblicate dai fornitori di microprocessori: Intel, AMD e ARM.

Guida per i clienti HPE

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

HPE consiglia a tutti i clienti di seguire la procedura qui riportata per determinare il livello e il piano di riduzione dei rischi.

1	2	3	4
			
Verifica se il tuo sistema è soggetto a questa vulnerabilità. HPE aggiorna costantemente l'elenco dei prodotti interessati sulla pagina del sito Web HPE dedicata alle vulnerabilità.	Se il tuo sistema è interessato, scarica e installa l'aggiornamento del sistema operativo pubblicato dal fornitore. In base al sistema utilizzato, puoi trovare istruzioni sulle azioni da intraprendere nel Bollettino di sicurezza HPE.	Aggiorna la ROM di sistema a una revisione contenente un microcodice aggiornato di HPE. In base al sistema utilizzato, puoi trovare istruzioni sulle azioni da intraprendere nel Bollettino di sicurezza HPE.	Riavvia il sistema come richiesto, verificando che i nuovi aggiornamenti siano correttamente installati.

Un aspetto importante del metodo di analisi side-channel è la presenza di malware in esecuzione sul sistema locale. Questa particolare vulnerabilità non consente processi diretti di alterazione, eliminazione, distruzione o crittografia dei dati, che potrebbero però venire estratti dai sistemi informatici. Di conseguenza, è importante rispettare le corrette prassi di sicurezza, 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 alla protezione dell'azienda da attacchi dannosi.

Gli aggiornamenti della ROM di sistema sono disponibili per gli attuali sistemi HPE Gen9 e Gen10. Prossimamente pubblicheremo gli aggiornamenti per i sistemi HPE Gen8 e le versioni precedenti.

Domande frequenti

1. **La vulnerabilità dei microprocessori riguarda tutti i fornitori del settore tecnologico o soltanto HPE?**
   La vulnerabilità dei microprocessori non riguarda soltanto HPE, ma l'intero settore. In assenza di una soluzione, è potenzialmente coinvolto ogni prodotto e soluzione che usa microprocessori con architetture moderne.

2. **Quali sono i prodotti e le soluzioni HPE interessati?**
   Tutti i prodotti HPE che contengano i microprocessori in questione sono potenzialmente vulnerabili. È disponibile un elenco di tali prodotti e soluzioni sulla pagina del sito Web HPE dedicata alle vulnerabilità. HPE aggiornerà l'elenco all'occorrenza.

3. **La vulnerabilità dei microprocessori è dovuta a un attacco o a una violazione in atto?**
   No, non c'è stato un attacco effettivo. La vulnerabilità è causata da un difetto di progettazione che, se analizzato tramite il metodo side-channel, può consentire ai malintenzionati di accedere ai dati. L'applicazione delle correzioni ai microprocessori, unita all'adozione dell'unica tecnologia Silicon Root of Trust originale, garantirà ai nostri clienti soluzioni HPE progettate per resistere a un eventuale attacco.

4. **Qual è la portata della vulnerabilità di sicurezza?**
   I nuovi studi sulla sicurezza descrivono metodi di analisi software che, se utilizzati da malintenzionati, possono raccogliere illecitamente 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. In base ai sistemi HPE utilizzati, puoi trovare istruzioni sulle azioni da intraprendere nel Bollettino di sicurezza HPE. Se sei un cliente HPE Pointnext e ritieni che il tuo sistema sia interessato dal problema, contatta il responsabile dell'assistenza.

6. **Quali sono i sistemi operativi coinvolti?**
   Windows, Linux e VMWare. I fornitori dei sistemi operativi stanno pubblicando i necessari aggiornamenti delle patch. Per ulteriori informazioni, HPE consiglia di contattarli direttamente: Microsoft, VMWare, SUSE e Red Hat.

7. **Quali sono i microprocessori interessati?**
   La maggior parte dei microprocessori con architetture moderne può essere soggetta al metodo di analisi side-channel. Intel e AMD hanno informato HPE di propria iniziativa e stanno collaborando attivamente per fornire le soluzioni necessarie. Contatta gli altri fornitori di microprocessori per ricevere ulteriori informazioni.

8. **Sono coinvolti altri produttori di hardware?**
   Tutti i produttori di hardware e i cloud pubblici che usano le moderne architetture dei microprocessori interessati sono potenzialmente vulnerabili. Sono coinvolti anche i telefoni cellulari e i computer client: rivolgiti ai relativi fornitori per maggiori dettagli.

9. **Dopo l'applicazione delle patch sui miei sistemi, ci saranno effetti sulle prestazioni?**
   Nella maggior parte dei casi, l'impatto sulle prestazioni sarà minimo, ma varierà in base al sistema operativo e al carico di lavoro. HPE e i suoi partner che si occupano di sistemi operativi e microprocessori lo esamineranno e forniranno ulteriori istruzioni in seguito.

10. **Che ripercussioni avrà questa vulnerabilità di sicurezza sui server HPE ProLiant e HPE Synergy Gen10, i server standard di settore più sicuri al mondo?**
    HPE produce i server standard di settore più sicuri al mondo. Questa particolare vulnerabilità riguarda i sistemi operativi e i microprocessori utilizzati nelle nostre soluzioni. Tuttavia, i server standard di settore HPE sono dotati dell'unica tecnologia Silicon Root of Trust originale: l'integrazione del nostro firmware nel silicio personalizzato di HPE assicura una protezione senza precedenti. Nonostante tali avanzate funzionalità di sicurezza, i clienti dovranno comunque applicare tutti gli aggiornamenti consigliati e seguire le best practice di sicurezza in relazione a questa particolare vulnerabilità.

11. **Che ripercussioni avrà questa vulnerabilità dei microprocessori sui clienti che valutano l'acquisto di prodotti HPE?**

    Possiamo garantire ai nostri clienti che le soluzioni di elaborazione HPE sono all'avanguardia in termini di sicurezza e qualità. La scoperta della falla dei microprocessori, che riguarda l'intero settore, non dovrebbe avere alcun impatto sulle decisioni di acquisto di 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 realizzate secondo i più elevati standard di sicurezza del settore.

12. **HPE fornirà altri aggiornamenti relativi a questa vulnerabilità?**
    Sì, HPE continuerà a pubblicare aggiornamenti non appena saranno disponibili ulteriori informazioni e dettagli. Puoi consultare il Bollettino per i clienti HPE.

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