Guida per l'utente di HP TamperLock

RIASSUNTO

HP TamperLock protegge da utenti malintenzionati che potrebbero aprire il case del PC e modificare l'hardware in maniera illecita.

Prima edizione: settembre 2020

Numero di parte del documento: M11669-061

Sommario

1 Panoramica 1

2 Funzionamento 2

3 Sequenza 3

4 Impostazioni dei criteri 4

5 Stato 6

Registro eventi 6

1 Panoramica

HP TamperLock protegge da utenti malintenzionati che potrebbero aprire il case del PC e modificare l'hardware in maniera illecita. HP TamperLock comprende sensori che rilevano se il case è stato aperto e controlli dei criteri per configurare quali azioni intraprendere in questa eventualità.

I criteri di HP TamperLock comprendono le capacità opzionali di blocco dell'avvio del sistema a livello di BIOS fino a quando non vengono immesse credenziali amministratore valide del BIOS; cancellazione del TPM (Trusted Platform Module) HP per eliminare tutte le chiavi utente (per esempio, le chiavi BitLocker che eseguono il rendering dei dati archiviati sull'unità locale accessibili solo tramite una chiave di ripristino BitLocker memorizzata in remoto); e la possibilità di spegnere il sistema immediatamente quando viene rimosso il coperchio. Gli eventi e la cronologia di apertura del coperchio sono memorizzati nell'hardware della piattaforma e un amministratore può eseguire una query da remoto.

I criteri di HP TamperLock sono protetti dalla modifica tramite un'archiviazione protetta con accesso root nell'hardware di HP Endpoint Security Controller. L'archiviazione protetta fornisce protezione da attacchi fisici per dati del firmware e BIOS e per le impostazioni memorizzate nella memoria flash in relazione alle impostazioni di HP TamperLock. Questa funzionalità è sempre presente sui sistemi che supportano HP TamperLock e non può essere disabilitata.

2 Funzionamento

La funzione HP TamperLock è configurata per bloccare il sistema in caso di accesso non autorizzato; rileva l'apertura del coperchio indipendentemente dallo stato di alimentazione del sistema quando si verifica un'apertura non autorizzata. In particolare, HP TamperLock rileva un evento di apertura del coperchio in tutti i seguenti stati di alimentazione del sistema quando HP TamperLock è configurato con le impostazioni consigliate da HP.

- **Sistema acceso** (sistema operativo [OS] in esecuzione)
- **Sistema spento** (arresto del sistema operativo o OS in ibernazione)
- **Sistema in sospensione**

IMPORTANTE: Per ottenere i risultati ottimali descritti in questo documento, configurare HP TamperLock con le impostazioni consigliate da HP, come mostrato nella Tabella 4-1.

Inoltre, il sensore di apertura del coperchio TamperLock HP si attiva anche in uno scenario in cui tutte le fonti di alimentazione sono rimosse mentre il coperchio viene rimosso, compresa la batteria interna e la batteria a bottone dell'orologio in tempo reale.

NOTA: La perdita di alimentazione dell'orologio in tempo reale attiva automaticamente la funzionalità del sensore di apertura del coperchio HP TamperLock. Pertanto, nel caso di sistemi che rimangono in deposito senza alcun alimentatore collegato per più di 2 anni, il sensore di apertura del coperchio HP TamperLock si attiverà anche quando il coperchio non è stato rimosso.

Quando HP TamperLock rileva un'apertura del coperchio mentre il sistema è acceso o in modalità sospensione, il sistema viene immediatamente spento e tutti i dati non salvati andranno perduti. Se il criterio facoltativo per cancellare lo stato del TPM sul rilevamento dell'apertura del coperchio è impostato su **Abilitato**, il BIOS cancella il TPM. Il BIOS non avvia il sistema operativo dopo che è stata rilevata un'apertura del coperchio, ma richiede all'utente locale di immettere la password amministratore del BIOS o (in modalità Sure Admin) un PIN monouso per sbloccare il sistema e avviarlo normalmente.

È possibile ottenere lo stato di HP TamperLock tramite una query dell'impostazione del BIOS associata o tramite il Visualizzatore eventi di Windows quando è installato il software HP Notifications.

3 Sequenza

La sequenza di HP TamperLock è descritta qui.

1. HP TamperLock rileva che il coperchio dello chassis è stato aperto.
2. Se il sistema è acceso o in modalità sospensione, HP TamperLock forza l'arresto senza possibilità di annullare.
3. L'evento di apertura del coperchio fa sì che l'hardware di sistema entri in uno stato di blocco.
4. Con il coperchio riposizionato, è possibile accendere nuovamente il sistema. Quando il sistema viene acceso nuovamente, si verificano i seguenti eventi:
    1. Se il criterio per cancellare il TPM è abilitato, il BIOS cancella il TPM.
    2. L'utente locale riceve una notifica dell'apertura del coperchio.
    3. Sono richieste le credenziali amministratore del BIOS:
        - Se vengono fornite le credenziali, il sistema si avvia normalmente.
        - Se le credenziali non vengono fornite, il sistema non avvia il sistema operativo.
5. La voce di registro di controllo viene sincronizzata con il registro eventi di Windows® se è installato il software HP Notifications.

4 Impostazioni dei criteri

È possibile utilizzare gli strumenti di HP Client Management per visualizzare e configurare i criteri di HP TamperLock come impostazioni del BIOS. Le impostazioni associate consentono di controllare l'abilitazione della funzionalità di HP TamperLock e le azioni intraprese quando il coperchio viene rimosso.

Tabella 4-1 Impostazioni dei criteri di TamperLock

Impostazioni	Descrizione	Predefinito	Consigliata da HP
Sensore di apertura del coperchio	• **Disabilitato**: non viene eseguita alcuna azione quando il coperchio viene rimosso. • **Notifica all'utente**: visualizza un messaggio di avviso all'avvio successivo se il coperchio è aperto. • **Credenziali amministratore**: questa impostazione richiede l'immissione della password amministratore o del PIN monouso (quando HP Sure Admin è abilitato) prima di continuare l'avvio dopo l'apertura del coperchio. Per abilitare questa impostazione, è necessario impostare una password o abilitare Enhanced BIOS Authentication Mode (Modalità di autenticazione BIOS avanzata) di HP Sure Admin con un set di chiavi di accesso locali. • **Password amministratore**: presenta lo stesso comportamento delle credenziali amministratore (il nome di questa impostazione è presente per mantenere la compatibilità con il software di gestione delle impostazioni precedente che supportava il sensore di apertura del coperchio).	Disabilitato	Credenziali amministratore o Password amministratore
Spegnimento all'apertura del coperchio	Disponibile solo se il sensore di apertura del coperchio non è impostato su Disabilitato. **Disabilitato**: se il sistema è acceso o in modalità sospensione quando il coperchio viene rimosso, rimane in tale stato. **Abilitato**: il sistema si spegne immediatamente se il coperchio viene rimosso mentre il sistema è acceso o in modalità sospensione (S3 o standby moderno).	Disabilitato	Abilitato
Cancellazione del TPM all'avvio dopo l'apertura del coperchio	Disponibile solo se il sensore di apertura del coperchio non è disabilitato. • **Disabilitato**: nessuna modifica allo stato del TPM quando viene rimosso il coperchio. • **Abilitato**: il TPM viene cancellato al successivo avvio dopo la rimozione del coperchio. Tutte le chiavi clienti nel TPM vengono cancellate.	Disabilitato	Dipende dai requisiti del cliente

Tabella 4-1 Impostazioni dei criteri di TamperLock (continuazione)

Impostazioni	Descrizione	Predefinito	Consigliata da HP
	NOTA: Abilitare questa impostazione solo quando è possibile eseguire il ripristino manuale dal backup remoto o quando non si desidera eseguire il ripristino. Se BitLocker è abilitato, l'unità non può essere decrittografata senza la chiave di ripristino BitLocker.		
Protezione DMA di pre-avvio	**Solo Thunderbolt**: la protezione DMA basata su hardware IOMMU (Input-Output Memory Management Unit) è abilitata in ambiente di preavvio del BIOS per i dispositivi PCIe collegati via Thunderbolt. **Tutti i dispositivi PCIe**: la protezione DMA basata su hardware IOMMU (Input-Output Memory Management Unit) è abilitata in ambiente di preavvio del BIOS per tutti i dispositivi interni ed esterni collegati via PCI.	Solo Thunderbolt	Tutti i dispositivi PCI
Protezione DMA	**Disabilitata**: il BIOS non configura l'hardware IOMMU (Input-Output Memory Management Unit) per l'utilizzo da parte dei sistemi operativi che supportano la protezione DMA. **Abilitata**: il BIOS configura l'hardware IOMMU (Input-Output Memory Management Unit) per l'utilizzo da parte dei sistemi operativi che supportano la protezione DMA.	Abilitata	Abilitata

5 Stato

È possibile eseguire una query dell'impostazione del BIOS per determinare lo stato di HP TamperLock utilizzando gli strumenti di gestione delle impostazioni del BIOS esistenti. L'unico modo per deselezionare questa impostazione è fornire la password amministratore del BIOS o le credenziali amministratore del BIOS (modalità Sure Admin).

Tabella 5-1

Impostazione	Descrizione
Ultima apertura coperchio e numero di aperture	Se il sensore di apertura del coperchio non è impostato su Disabilitato, questa impostazione riporta l'ultima volta che il coperchio è stato rimosso e il numero di volte in cui è stato rimosso e confermato dopo l'ultimo azzeramento dell'amministratore del BIOS. Il formato è MM/DD/YYYY HH:MM:SS. X times. A seconda dei fattori di sistema (per esempio se il computer è spento), aperture consecutive del coperchio non incrementeranno il numero di aperture. La data e l'ora vengono indicate con tutti zeri nei casi in cui non sia possibile determinare il valore, per esempio dopo una perdita di potenza dell'orologio in tempo reale.

Registro eventi

Se è installato il software HP Notifications, è possibile visualizzare i seguenti registri eventi nel Visualizzatore eventi di Windows nella cartella HP Sure Start.

Tabella 5-2 Registro di controllo

ID origine	ID evento	Evento	Tipo di registro eventi
0x8A	0x1E	HP TamperLock - Il sistema ha rilevato che il coperchio è stato aperto.	Avvertenza
	0x1F	HP TamperLock - L'utente ha confermato una notifica POST del BIOS relativa all'apertura del coperchio.	Informativo
	0x20	HP TamperLock - Il TPM è stato cancellato a causa dell'apertura del coperchio in base alle impostazioni correnti dei criteri di HP TamperLock.	Informativo