

VM escape su VMware Workstation e Fusion: cosa cambia per i laboratori di analisi malware

Il 3 settembre 2026 Broadcom ha pubblicato il bollettino VMSA-2026-0007. Corregge due vulnerabilità di VM escape, cioè di fuga dalla macchina virtuale, in VMware Workstation e Fusion: una di gravità critica e una di gravità alta. Lo stesso giorno il CSIRT Italia ha diffuso l'alert AL03/260903/CSIRT-ITA, con impatto sistemico stimato "Alto" (65,76). Per la maggior parte delle organizzazioni è un ordinario aggiornamento. Per chi lavora in un laboratorio di analisi malware o in una postazione di informatica forense il problema è diverso. Workstation e Fusion sono lo strumento con cui, ogni giorno, si esegue codice ostile di proposito, confidando che resti confinato. Le due falle mettono in discussione proprio quel confine.

1. Le due vulnerabilità in sintesi

Le due vulnerabilità colpiscono componenti diversi dell'hypervisor, ma condividono il modello di minaccia: un attaccante con privilegi amministrativi dentro la macchina virtuale ottiene esecuzione di codice sul sistema ospitante.

CVE-2026-59346 è un integer overflow nel controller di rete virtuale VMXNET3. Broadcom la classifica come critica, con punteggio CVSSv3 massimo di 9,3. Secondo il bollettino, un attaccante con privilegi amministrativi locali su una macchina virtuale dotata di adattatore VMXNET3 può sfruttarla per eseguire codice sull'host. L'hanno segnalata, in modo indipendente, un ricercatore di secsys lab e due ricercatori che collaborano con la Zero Day Initiative (indicata nel

bollettino come “TrendAI Zero Day Initiative”).

CVE-2026-59347 è uno stack buffer overflow in HGFS (Host-Guest File System), il meccanismo delle cartelle condivise tra guest e host. Il punteggio è 8,1 e la gravità è “importante”. Nella scala VMware il termine corrisponde alla fascia “alta” di FIRST, tra 7,0 e 8,9. Lo sfruttamento consente di eseguire codice con i privilegi del processo VMX della macchina virtuale sull’host. L’hanno segnalata due ricercatori del Tencent Xuanwu Lab.

Le versioni interessate sono la 25H2 e la 26H1, sia di Workstation (su qualsiasi sistema operativo host) sia di Fusion (su macOS). La correzione è nella versione 26H1u1, rilasciata il 3 settembre per entrambi i prodotti. Le note di rilascio indicano la build 25688693 per Workstation Pro e la build 25689522 per Fusion Pro.

Broadcom indica che non esistono misure alternative all’aggiornamento. Il dato va letto insieme alla politica di risposta VMware: per le vulnerabilità di gravità critica il produttore si impegna a cercare una modifica di configurazione che chiuda i vettori di attacco noti. Per CVE-2026-59346, che rientra in quella fascia, la ricerca non ha dato esito.

Un dettaglio tecnico merita attenzione. Il vettore CVSS di CVE-2026-59346 indica complessità di attacco bassa (AC:L); quello di CVE-2026-59347 indica complessità alta (AC:H). In termini pratici, la falla su VMXNET3 è quella più facile da trasformare in un codice di attacco funzionante. Entrambi i vettori riportano un cambio di ambito (S:C), coerente con un impatto che supera il perimetro del componente vulnerabile.

Sullo sfruttamento, il bollettino descrive entrambe le vulnerabilità come segnalate privatamente e non contiene note su attacchi osservati. Il silenzio ha un peso: la politica VMware prevede che i bollettini riportino in nota la conferma di sfruttamento, quando esiste. L’alert del CSIRT Italia, al 3

settembre, non registra né codice di attacco pubblico né sfruttamento. Alla data di pubblicazione di questo articolo, la scheda di CVE-2026-59346 su cve.org risulta ancora nello stato “reserved”, cioè priva di dettagli tecnici. È una fotografia del momento, non una garanzia: i precedenti insegnano che la situazione può cambiare in fretta.

2. Perché l'isolamento della VM non è un confine di sicurezza

La virtualizzazione desktop nasce per far convivere sistemi diversi sulla stessa macchina, non per contenere un avversario. L'isolamento tra guest e host è un effetto utile dell'architettura. Poggia però su decine di migliaia di righe di codice che emulano dispositivi: schede di rete, controller di archiviazione, schede grafiche, canali di comunicazione con l'host. Ogni dispositivo emulato è una superficie che il guest può sollecitare con dati arbitrari.

Le due falle di settembre colpiscono esattamente questo strato. VMXNET3 è un dispositivo di rete paravirtualizzato: il guest gli invia descrittori di pacchetti che il processo VMX sull'host deve interpretare. HGFS è un protocollo di condivisione file: il guest formula richieste che l'host esegue sul proprio file system. In entrambi i casi il codice che elabora i dati provenienti dal guest gira sull'host, con i privilegi del processo VMX.

Non è un caso isolato. La sequenza degli ultimi diciotto mesi lo mostra.

Nel marzo 2025 il bollettino VMSA-2025-0004 aveva corretto tre vulnerabilità in ESXi, Workstation e Fusion. La prima era un heap overflow nel componente VMC1 (CVE-2025-22224, anch'esso a 9,3); la seconda una scrittura arbitraria in ESXi (CVE-2025-22225); la terza una lettura fuori limite proprio in HGFS (CVE-2025-22226). Le aveva segnalate il Microsoft Threat

Intelligence Center. Broadcom dichiarò di avere informazioni su uno sfruttamento già avvenuto per almeno le prime due. CISA inserì le tre CVE nel catalogo KEV lo stesso 4 marzo, con scadenza di rimedio al 25 marzo. Per CVE-2025-22225 il catalogo registra oggi anche l'uso in campagne ransomware. Il modello di attacco era lo stesso di oggi: privilegi amministrativi nel guest, esecuzione di codice come processo VMX sull'host.

Il 29 luglio 2026 il bollettino VMSA-2026-0006 ha corretto, tra le altre, CVE-2026-47876. È una scrittura fuori limite nell'adattatore VMXNET3 di ESX, anch'essa a 9,3 e senza misure alternative. Il vettore di attacco è lo stesso: privilegi amministrativi in un guest con VMXNET3, esecuzione di codice sull'host. La falla era emersa alla competizione Pwn2Own tramite un ricercatore di STARLabs SG. Lo stesso bollettino correggeva in Workstation e Fusion 25H2 una lettura fuori limite (CVE-2026-41703), con impatto limitato alla divulgazione di informazioni. Cinque settimane dopo, lo stesso adattatore virtuale torna al centro di un bollettino, questa volta sui prodotti desktop.

La conclusione operativa è semplice da enunciare e scomoda da applicare. Un hypervisor di tipo 2, che gira come applicazione sopra un sistema operativo generico, offre un isolamento probabilistico, non un confine di sicurezza garantito. Va trattato come tale.

3. Il caso dei laboratori di analisi malware

Un laboratorio di analisi dinamica è, per definizione, l'ambiente in cui il modello di minaccia del bollettino si realizza per scelta. Il campione viene eseguito nel guest, spesso con privilegi amministrativi, perché è così che si osserva il comportamento completo di un malware. Il requisito "attaccante con privilegi amministrativi nella macchina

virtuale" non va conquistato: è la configurazione di partenza.

Un elemento di contesto: Workstation Pro e Fusion Pro sono gratuiti anche per uso commerciale ed educativo, senza chiave di licenza, come ricordano le note di rilascio. È ragionevole attendersi che questo abbia abbassato la soglia di adozione anche per piccole strutture, studi di consulenza e corsi universitari, dove la gestione degli aggiornamenti è meno strutturata.

Alcune configurazioni ricorrenti in questi ambienti amplificano il rischio:

- **Cartelle condivise attive.** HGFS è comodo: si trascina il campione nella cartella condivisa e si raccolgono i registri e gli artefatti nella stessa cartella. Ma ogni cartella condivisa è un canale bidirezionale tra guest e host, ed è precisamente il componente colpito da CVE-2026-59347.
- **Adattatore VMXNET3 come predefinito.** Molte immagini di laboratorio nascono da modelli che usano VMXNET3 per le prestazioni. Se il laboratorio simula la rete con strumenti come INetSim o FakeNet-NG per osservare il traffico del campione, l'adattatore è attivo e sollecitato.
- **Snapshot come unica difesa.** Il flusso "esegui, osserva, ripristina lo snapshot" protegge il guest, non l'host. Se il campione è uscito dalla macchina virtuale, il ripristino cancella le tracce nel guest e lascia intatta la compromissione sull'host.
- **Strumenti sensibili sulla stessa macchina.** Sulla postazione dell'analista convivono spesso credenziali di piattaforme di threat intelligence, chiavi di accesso ad archivi di codice interni, client di posta, connessioni VPN verso la rete aziendale. Una fuga dalla VM non colpisce una macchina qualsiasi, ma una delle più ricche di accessi dell'intera organizzazione.

Va detto che il malware con capacità di VM escape resta raro: la maggior parte dei campioni si limita a rilevare la virtualizzazione e a cambiare comportamento. Ma la valutazione va fatta sul campione peggiore, non su quello medio. Un laboratorio che analizza attività di gruppi strutturati, o campioni ricevuti durante un incidente in corso, deve considerare l'ipotesi che l'avversario conosca queste falle prima che siano pubbliche.

4. Informatica forense: integrità dell'ambiente e catena di custodia

Il risvolto forense è il più delicato, perché sposta il problema dal piano tecnico a quello processuale, dove contano integrità della prova e catena di custodia.

Contaminazione dell'ambiente di analisi. Molti consulenti tecnici usano Workstation o Fusion per esaminare immagini forensi. Si monta la copia del disco in una macchina virtuale, oppure si avvia direttamente l'immagine per ricostruire l'operatività del sistema. Se il sistema esaminato contiene codice malevolo capace di VM escape, la postazione forense diventa un sistema compromesso. Da quel momento ogni strumento in esecuzione sull'host, compresi quelli di acquisizione e di calcolo degli hash, opera su una piattaforma di cui non si può più garantire l'integrità.

Ripetibilità dell'accertamento. L'articolo 360 del codice di procedura penale disciplina gli accertamenti tecnici non ripetibili, con garanzie di partecipazione per la difesa. Un accertamento condotto su una piattaforma compromessa può essere contestato come non ripetibile nelle medesime condizioni, perché lo stato dell'ambiente di analisi non è documentato né ricostruibile. Questa è un'interpretazione di chi scrive, non un orientamento giurisprudenziale consolidato; è però un argomento che una difesa attenta può sollevare.

Conservazione dei dati originali. La legge 18 marzo 2008, n. 48, che ha ratificato la Convenzione di Budapest, ha modificato con il Capo III il codice di procedura penale (D.P.R. 22 settembre 1988, n. 447). Tre articoli, sulle ispezioni (244, comma 2), sulle perquisizioni disposte dall'autorità giudiziaria (247, comma 1-bis) e su quelle di iniziativa della polizia giudiziaria (352, comma 1-bis), usano la stessa formula: le operazioni sui sistemi informatici vanno svolte "adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione". L'articolo 354, comma 2, sugli accertamenti urgenti, va oltre: la polizia giudiziaria deve impedire l'alterazione e l'accesso ai dati e provvedere, ove possibile, alla loro duplicazione immediata "mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità". La stessa esigenza torna nell'articolo 260, comma 2, per la copia dei dati sequestrati. Il legislatore, in altre parole, chiede integrità e immodificabilità della copia: proprietà che presuppongono una piattaforma di acquisizione non compromessa.

Lo standard ISO/IEC 27037:2012 va nella stessa direzione per le fasi di identificazione, raccolta, acquisizione e conservazione della prova digitale. Va precisato che la norma esclude espressamente la fase di analisi e non impone strumenti specifici: la credibilità dell'accertamento poggia sulla metodologia applicata e sulla qualificazione di chi la esegue. Tre definizioni della norma sono utili qui. La ripetibilità (punto 3.17) è la proprietà di un processo di dare gli stessi risultati nello stesso ambiente di prova: stesso computer, stesso disco, stessa modalità operativa. La riproducibilità (3.18) è la proprietà di dare gli stessi risultati in un ambiente di prova diverso. La spoliazione (3.19) è ogni modifica alla prova, provocata o anche solo consentita, che ne riduce il valore probatorio. Un consulente può sostenere che un hypervisor con una vulnerabilità nota e non corretta incrina tutte e tre: l'ambiente di prova non è

più documentabile come stabile, e una fuga dal guest è una modifica consentita per omissione. Anche questa è una lettura interpretativa, non una posizione espressa dalla norma.

Documentazione nel verbale. La contromisura documentale non ha costi e va adottata subito. Nel verbale di acquisizione o nella relazione tecnica vanno riportati: prodotto, versione e build dell'hypervisor (per esempio "VMware Workstation Pro 26H1u1, build 25688693"); data dell'ultimo aggiornamento; configurazione della macchina virtuale, con adattatore di rete, cartelle condivise e strumenti di integrazione guest attivi. Se l'accertamento è avvenuto su una versione vulnerabile prima della pubblicazione del bollettino, è preferibile darne atto spontaneamente. L'alternativa è che lo scopra la controparte.

5. Buone pratiche di laboratorio

L'aggiornamento alla 26H1u1 è il primo passo, non l'ultimo. Le misure che seguono riducono la superficie esposta anche alle vulnerabilità future di questa classe:

1. **Separazione fisica per i campioni ad alto rischio.** Per campioni attribuiti a gruppi strutturati, o ricevuti durante un incidente attivo, la scelta più prudente resta la macchina fisica dedicata e isolata dalla rete. Un hypervisor di tipo 1 su hardware dedicato, senza dati sensibili a bordo, è una soluzione intermedia accettabile ma non risolutiva: la falla di luglio su ESX ricorda che anche quel livello ha le sue vulnerabilità.
2. **Disattivazione di HGFS e delle cartelle condivise.** Nelle macchine di analisi le cartelle condivise vanno disattivate per impostazione predefinita. Il trasferimento dei campioni può avvenire tramite immagine ISO montata in sola lettura; la raccolta degli artefatti tramite esportazione del disco virtuale dopo lo spegnimento.

3. **Rimozione delle interfacce non necessarie.** Se il campione non ha bisogno di rete, l'adattatore va rimosso, non solo disconnesso. Lo stesso vale per audio, USB, accelerazione 3D e appunti condivisi. Ogni dispositivo emulato in meno è codice del processo VMX che il guest non può sollecitare. Sostituire VMXNET3 con un adattatore emulato non è una difesa strutturale: il bollettino di luglio precisa che gli altri adattatori non sono interessati da quella specifica falla, ma non presenta il cambio di adattatore come misura alternativa.
4. **Nessuna credenziale sull'host di analisi.** La postazione che ospita il laboratorio non deve contenere accessi a sistemi aziendali, piattaforme di threat intelligence o archivi di codice. Se una fuga avviene, deve trovare un host povero.
5. **L'hypervisor come bene critico nella gestione delle vulnerabilità.** Workstation e Fusion vanno censiti e trattati con le stesse tempistiche di un sistema esposto, non come software da ufficio. L'assenza di misure alternative in questo bollettino rende il ritardo nell'aggiornamento una scelta consapevole di esposizione. La gratuità del prodotto non lo rende meno critico: lo rende più diffuso.
6. **Verifica dell'host dopo ogni sessione ad alto rischio.** Il ripristino dello snapshot non basta. Dopo l'analisi di un campione classificato ad alto rischio, l'host va sottoposto a controlli di integrità: processi in esecuzione, connessioni di rete, meccanismi di persistenza, confronto con uno stato di riferimento noto.

6. Cosa chiedere ai fornitori di

servizi di analisi e perizia

Chi affida all'esterno l'analisi di campioni o la perizia su dispositivi ha titolo per porre domande precise. Non serve competenza tecnica per formularle, e le risposte dicono molto sulla maturità del fornitore:

- Quale hypervisor usate per l'analisi dinamica e in quale versione? Con quali tempi applicate i bollettini di sicurezza del produttore e gli alert del CSIRT Italia?
- I campioni ad alto rischio vengono analizzati su infrastruttura separata da quella che ospita dati di altri clienti?
- Le cartelle condivise e gli strumenti di integrazione tra guest e host sono disattivati nelle macchine di analisi?
- Versione e build dell'hypervisor e configurazione della macchina virtuale sono documentate nel verbale o nella relazione tecnica?
- Cosa prevede la vostra procedura in caso di compromissione della postazione di analisi, e come ne date comunicazione al cliente?

Un fornitore che risponde con precisione a queste domande ha già affrontato il problema.

Conclusione

Le due vulnerabilità corrette da VMSA-2026-0007 verranno chiuse dall'aggiornamento nella maggior parte degli ambienti. La lezione per i laboratori di analisi e per le postazioni forensi è invece durevole. Tre bollettini in diciotto mesi, con lo stesso modello di attacco, mostrano che l'isolamento di una macchina virtuale è una proprietà del software, con i difetti del software. Chi esegue codice ostile per mestiere deve progettare l'ambiente sapendo che, prima o poi, quel confine verrà attraversato.

<https://www.ictsecuritymagazine.com/notizie/vm-escape-vmware-workstation/>