

Zero-day Magento e Adobe Commerce: StyleSmuggler sfruttato attivamente, Adobe non ha ancora rilasciato la patch

Dal 4 settembre 2026 un attacco senza correzione ufficiale colpisce i negozi Magento Open Source aggiornati. Le mitigazioni disponibili sono di terze parti. Per gli e-commerce italiani si aprono due questioni giuridiche: la notifica al Garante e la responsabilità dell'agenzia.

Dal 4 settembre 2026 gli e-commerce basati su Magento Open Source e Adobe Commerce sono esposti a un attacco attivo. Il produttore non ha ancora pubblicato una correzione. La vulnerabilità, chiamata **StyleSmuggler** dalla società olandese Sansec che l'ha scoperta, permette a un attaccante non autenticato di eseguire codice sul server del negozio e di installare una backdoor persistente.

Al 6 settembre Adobe non ha pubblicato avvisi, identificativi CVE, patch o soluzioni temporanee. L'indice dei bollettini di sicurezza di Adobe Commerce si ferma all'aggiornamento dell'11 agosto (APSB26-92). Quel bollettino correggeva sette CVE, tra cui un'escalation di privilegi non autenticata con punteggio CVSS 9.1 (CVE-2026-71362), e dichiarava che Adobe non era a conoscenza di exploit in circolazione. Secondo Sansec, la prossima release di sicurezza è prevista per l'8 settembre, ma non è noto se coprirà questo difetto.

Questo articolo non ripercorre la cronaca. Si concentra sul vuoto tra la scoperta e la patch. Cosa può fare oggi un esercente italiano che tratta dati di pagamento? Quali limiti

hanno le mitigazioni non ufficiali? Quali obblighi giuridici scattano quando la compromissione è probabile ma non accertata?

Cosa è StyleSmuggler

La cronologia dell'avviso di Sansec fissa la prima esecuzione confermata dell'exploit alle 22:20 UTC del 4 settembre. Alle 22:40 Sansec ha individuato la campagna; alle 23:10 il suo scanner eComscan ha segnalato l'impianto su negozi non collegati tra loro. Nelle ore successive Sansec ha riprodotto l'intera catena su installazioni pulite di Magento Open Source 2.4.7, 2.4.8 e 2.4.9. Le regole di blocco del suo prodotto Shield sono entrate in funzione il 5 settembre alle 07:15 UTC. L'avviso è uscito lo stesso giorno, prima del completamento dell'analisi, perché i negozi venivano compromessi in quel momento.

L'attacco abusa del sistema di template di Magento, in particolare delle proprietà styles, per aggirare le protezioni esistenti. Si svolge in due fasi:

1. **Iniezione.** L'attaccante fa scrivere codice PHP in un file che Magento stesso genera. Sansec cita i rapporti di errore in var/report/. Disrex Group, società olandese di hosting e sviluppo Magento, ha gestito la risposta a due negozi compromessi. In entrambi i casi ha osservato l'avvelenamento di var/log/system.log: l'attaccante invia un codice negozio non valido e Magento lo registra così com'è. Secondo Disrex questa fase non è filtrabile a livello di server web, perché è indistinguibile da un'integrazione malfunzionante.
2. **Esecuzione.** L'attaccante provoca l'invio dell'email standard "Payment Transaction Failed Reminder". Il codice iniettato viene eseguito mentre Magento prepara il messaggio. Nessuno deve aprire l'email; l'attacco riesce anche se la consegna fallisce. L'assenza di

messaggi in casella non è quindi una prova di sicurezza.

La ricostruzione del meccanismo, pubblicata da Disrex in un documento dedicato, è un'interpretazione indipendente. Secondo questa lettura, una direttiva `{{block}}` nel testo iniettato conduce, attraverso una catena di classi native di Magento, fino a codice pensato per il solo compilatore di dependency injection da riga di comando. Quel codice termina con un `include` su un percorso scelto dall'attaccante: il log avvelenato un istante prima. Disrex ha corretto una prima versione che identificava un punto di ingresso sbagliato. Sansec non ha confermato la ricostruzione né pubblicato la catena completa; Disrex non ha diffuso la richiesta assemblata. Per le stesse ragioni questo articolo non riporta dettagli riproducibili.

Una volta ottenuta l'esecuzione, un dropper PHP prova in ordine sei funzioni di avvio processo (`shell_exec`, `exec`, `system`, `passthru`, `proc_open`, `popen`) e usa la prima disponibile. Poi scarica e avvia l'impianto: un binario Rust statico e privo di simboli di circa 1,9 MB, per x86-64 e arm64. Il file viene installato in `~/.local/share/.gvfsd/gvfsd-user`, nella home dell'utente del sito e non nella cartella web. Il processo si maschera con il nome `[kworker/u:8:0]`, tipico di un thread del kernel Linux. Una voce cron lo riavvia ogni cinque minuti; è scritta direttamente nel file di spool, così il registro di sistema non mostra alcuna sostituzione del crontab.

Il perimetro reale: perché le patch di agosto non proteggono

Il dato che più dovrebbe preoccupare i responsabili IT è il profilo della prima vittima documentata da Sansec. Girava su Magento 2.4.6-p15, con le patch di luglio e agosto 2026 applicate e `security:patch-status` pulito. È il livello più alto che Adobe distribuisce per la linea 2.4.6, quello che il

bollettino di agosto etichetta 2.4.6-2026-aug. Secondo la cronologia delle versioni, il supporto ordinario di quella linea è terminato l'11 agosto 2026, con supporto esteso fino ad agosto 2027. Essere aggiornati non ha protetto.

Il secondo caso documentato è l'opposto. Il negozio 2.4.7-p2 gestito da Disrex girava su un livello del 13 agosto 2024, otto livelli indietro rispetto al 2.4.7-p10 del 12 maggio 2026. L'esito è stato lo stesso. Come scrive Disrex, il livello di patch non dice nulla sull'esposizione.

Il perimetro noto al 6 settembre è il seguente:

- **Vulnerabile per riproduzione diretta:** Magento Open Source 2.4.7, 2.4.8, 2.4.9 (Sansec).
- **Compromesso in attacchi reali:** 2.4.6-p15 (Sansec), 2.4.7-p2 (Disrex).
- **Non verificato:** Adobe Commerce e Adobe Commerce on Cloud. L'avviso Sansec li dichiara interessati, ma riporta riproduzioni solo su Magento Open Source. Adobe non ha confermato quali versioni siano coinvolte. Vanno trattate come esposizione sconosciuta, non come sicure.
- **Fuori perimetro:** Magento 1, fuori supporto dal 2020. Non esistono dati e le mitigazioni descritte più avanti non sono state provate.

La cronologia di Disrex aggiunge un elemento che va oltre il caso specifico. Il suo primo negozio è stato colpito alle 23:10 UTC del 4 settembre, cinquanta minuti dopo la prima esecuzione confermata a livello mondiale e otto ore prima che esistesse qualsiasi regola di blocco. Nessun livello di patch e nessuna firma avrebbero coperto quella finestra. È l'argomento più forte a favore delle misure di sistema indipendenti dalla vulnerabilità, descritte più avanti.

Non esistono statistiche ufficiali sulla diffusione di Magento in Italia. Chi voglia stimare l'esposizione nazionale può usare servizi di rilevamento tecnologico come BuiltWith o

W3Techs con filtro geografico. Questi strumenti contano i domini, non le installazioni, e non distinguono in modo affidabile Open Source da Adobe Commerce. La domanda pratica è un'altra: il mio sito espone l'endpoint /graphql e quale vetrina lo usa? Vale anche ricordare che StyleSmuggler non è un caso isolato. A giugno una falla nel modulo di terze parti Mirasvit Full Page Cache Warmer (CVE-2026-45247), segnalata in questa rassegna, apriva anch'essa a esecuzione di codice remota non autenticata sui negozi Magento e Adobe Commerce, ed è stata inserita da CISA nel catalogo delle vulnerabilità sfruttate. La differenza è che StyleSmuggler colpisce il core della piattaforma, non un'estensione, e non ha una patch.

Indicatori di compromissione e verifica

Il primo passo, prima di qualsiasi mitigazione, è verificare se il negozio è già compromesso. Applicare regole di blocco su un server infetto non serve: l'impianto è dentro e si riavvia da solo.

Gli indicatori pubblicati da Sansec e nell'elenco di Disrex, aggiornato nel corso del 5 settembre, convergono su questi elementi:

- **Processo:** [kworker/u:8:0] di proprietà di un utente non root. Un vero thread del kernel appartiene sempre a root e non ha memoria residente. Un nome tra parentesi quadre sull'utente del sito, con memoria reale, è l'impianto. L'impianto imposta la riga di comando alla stringa letterale, quindi un controllo sul campo comm del processo non trova nulla; va letto args.
- **File:** `~/.local/share/.gvfsd/gvfsd-user,`
`~/.local/share/.gvfsd/.gvfsd_<8hex>.lock,`
`/tmp/.gvfsd_<8hex>.lock, /tmp/.kw_<random>.`
- **Cron:** `*/5 * * * * exec <home>/.local/share/.gvfsd/gvfsd-user,` con una variante che punta a `/tmp/.kw_`. Su un

negozio la stessa riga compariva 1.728 volte e tornava entro un secondo dalla rimozione.

- **Hash SHA-256:** Sansec pubblica due campioni (e315687a...a26a7 e b79dfdc1...51420). Disrex ne aggiunge uno trovato su disco in entrambi i negozi (8334b434...d06ef) e uno diverso in esecuzione in memoria su uno di essi (251fabd5...bf220). L'operatore aggiorna l'impianto in memoria: va calcolato l'hash anche di /proc/<pid>/exe.
- **Rete:** 247.cdnflare[.]xyz (host di scaricamento), 99.84.67[.]186:443 (comando e controllo via WebSocket su TLS), windwsecurity[.]run:443 (shell remota). Tre domini imitano server NTP con traffico UDP sulla porta 123: ntp.timesysnc[.]net, time.microsoft[.]run, pool.microsoft[.]studio. Le imitazioni di Microsoft sono evidenti e vanno cercate nei log DNS.
- **Sorgenti:** 88.216.72[.]181 (Sansec, vista su più vittime), 5.181.86[.]133 e 91.238.181[.]19 (Disrex, traffico in massa). La seconda è la sorgente quasi esclusiva della seconda ondata, nel pomeriggio del 5 settembre.
- **Firme di richiesta:** POST /graphql?styles[...]= con codifica percentuale; POST /paypal/transparent/response/ con codice PHP nella stringa di query. C'è poi la richiesta ordinaria GET /customer/section/load/, che nella variante osservata da Disrex portava il payload nell'intestazione User-Agent. Le richieste di exploit arrivano con user agent python-requests (2.15.0 nella prima ondata, 2.32.4 nella seconda), mai con un browser.
- **Prova di esecuzione:** secondo Disrex il payload racchiude il proprio output in un delimitatore MG<20 hex>::...::/MG<20 hex>. La sua presenza nei log prova che il codice è stato eseguito, non solo inviato. Un secondo segnale è un TypeError di array_merge() con argomento intero in system.log, subito dopo l'include: indica che l'exploit è riuscito. La variante più silenziosa restituisce un array vuoto e non lascia

traccia.

Tre avvertenze emerse sul campo meritano attenzione. Primo: il controllo pubblicato da Sansec cerca X_TRACE_ in var/report/. Entrambe le infezioni gestite da Disrex passavano da var/log/system.log e sarebbero sfuggite; vanno ispezionate entrambe le cartelle. Secondo: l'intestazione di innesco è cambiata nella stessa giornata, da X-TRACE-<10 hex> al mattino a X-<12 hex> al pomeriggio, con valore rigenerato a ogni richiesta. Una rilevazione ancorata alla stringa letterale è diventata cieca in un giorno: la ricerca deve intercettare la forma. Terzo: su uno dei due negozi l'impianto non ha aperto alcuna connessione in uscita. Ha letto le sessioni Magento dall'istanza Redis locale con 28 connessioni a 127.0.0.1:6379. Due catture di traffico di oltre 200 MB ciascuna non contenevano un solo pacchetto verso gli indirizzi noti. L'assenza di traffico sospetto non prova nulla.

Sugli scanner c'è un dato discordante, da riportare come tale. Sansec raccomanda il proprio eComscan e ha rilasciato la versione 1.9.7, che termina i processi per i clienti Shield. Disrex riferisce invece che su uno dei negozi infetti lo scanner, con i controlli su processi in background e attività pianificate attivi, ha dato esito pulito con 1.728 righe cron malevole presenti. Disrex non indica versione e orario dell'esecuzione. In ogni caso gli scanner puntati sulla sola cartella web non vedono un impianto installato un livello sopra.

Un segnale indiretto: raffiche inattese di email "Payment Transaction Failed Reminder" sono un motivo per indagare, anche se pagamenti rifiutati legittimamente generano la stessa notifica.

Mitigazioni disponibili ora

In assenza di una correzione del produttore, le opzioni si dispongono su tre livelli. L'ordine riflette la robustezza. La

ragione sta nella struttura della catena come la descrive Disrex. Il punto di ingresso non può essere protetto in modo pulito, perché il codice che elabora il testo iniettato prepara anche ogni email transazionale. Un controllo lì romperebbe le conferme d'ordine. Restano il blocco del punto di uscita e le misure che non dipendono dalla conoscenza della vulnerabilità.

Livello 1: misure di sistema indipendenti dalla catena. Sono le due misure che Disrex mette davanti a ogni altra regola del proprio repository. Su uno dei negozi compromessi le prime quattro delle sei funzioni tentate dal dropper erano disabilitate, ma `proc_open` no. È stata quella ad avviare l'impianto, e `open_basedir` non ha contenuto il processo figlio, che una volta avviato gira fuori da PHP. Una lista `disable_functions` che ferma cinque funzioni su sei non ferma nulla. Le misure sono quindi due: aggiungere `proc_open` e le altre cinque funzioni a `disable_functions` in PHP; montare `/tmp`, `/var/tmp` e `/dev/shm` con opzione `noexec`, così che un binario scaricato non possa essere eseguito. Entrambe vanno provate in staging, perché alcune estensioni legittime dipendono da `proc_open`.

Livello 2: disattivazione temporanea di GraphQL. È il consiglio interinale di Sansec per i negozi che non usano Shield. Le vetrine headless e PWA richiedono GraphQL; la maggior parte delle vetrine classiche e Hyvä non lo usa. Un conteggio delle richieste `POST /graphql` nei log di accesso dice se la disattivazione è praticabile. È la strada scelta anche da alcuni fornitori di hosting. Nexcess, marchio di Liquid Web, ha comunicato la sera del 5 settembre un blocco completo delle richieste GraphQL su tutti gli ambienti Magento e Adobe Commerce gestiti. Ha avvertito che le vetrine headless e PWA possono risentirne. Un esercente italiano su hosting gestito potrebbe quindi trovarsi con GraphQL bloccato senza averlo deciso: va verificato con il fornitore.

Livello 3: patch e regole non ufficiali. Tre soggetti hanno

pubblicato mitigazioni il 5 settembre:

- **Disrex Group** ha rilasciato regole nginx e Apache che bloccano le richieste con i parametri dell'exploit nella stringa di query. Ha pubblicato inoltre un guard per tre metodi degli scanner di dependency injection di Magento (ArrayScanner, ClassesScanner, XmlInterceptorScanner), che impedisce loro di girare fuori dalla riga di comando. Il guard è disponibile anche come patch composer che si riapplica a ogni deploy. Secondo Disrex, la patch è stata verificata in prova a secco sui tag 2.4.6, 2.4.7, 2.4.8 e 2.4.9. È stata poi applicata su installazioni attive 2.4.7-p2 e 2.4.8-p4, con setup:di:compile e vetrina funzionanti. Il repository dichiara i propri limiti. È stato scritto con assistenza di intelligenza artificiale durante un incidente e non è stato revisionato. Le regole Apache non sono mai state eseguite su un server Apache reale; nulla è stato provato su hosting condiviso, Docker o pannelli di controllo. Una prova su un negozio attivo ha mostrato che le regole per il server web si aggirano spostando gli stessi parametri nel corpo di una POST. Fermano la campagna come è condotta oggi, non la vulnerabilità. Disrex avverte che il guard non è una correzione completa, perché in Magento esistono altri punti di include non proteggibili allo stesso modo.
- **ProxiBlue** ha pubblicato su GitHub tre patch con lo stesso guard sugli stessi tre metodi, in modo indipendente. Disrex le cita come conferma incrociata e raccomanda di applicare una sola delle due soluzioni.
- **Graycore LLC** ha pubblicato un modulo Magento su GitHub e Packagist che irrobustisce tre punti della catena. La direttiva `{{block}}` dei template email rifiuta i blocchi di backend. Il generatore di URL delle righe di griglia valida la classe prima di costruirla. I tag di apertura PHP nei rapporti di errore delle Web API vengono spezzati. L'ultima release (2.0.0) aggiunge il rifiuto

di template caricati da stream wrapper o percorsi con byte nullo e rimuove un override di un resolver PayPal presente nella prima versione. L'autore avverte che il pacchetto cambierà mentre prova nuovi livelli di mitigazione e che va letto il changelog prima di ogni aggiornamento. Precisa che si tratta di irrobustimento e non di correzione: la vulnerabilità resta aperta.

Va detto con chiarezza: né Sansec né Adobe hanno confermato che gli scanner DI siano il punto in cui la catena termina. Chi applica queste patch lo fa a proprio rischio, sulla base di una ricostruzione indipendente non convalidata dal produttore.

Se il negozio è già compromesso. La guida di pulizia di Disrex fissa un ordine. Prima confermare e preservare le prove; poi contenere, cercare altre persistenze e ruotare i segreti; quindi decidere se pulire o ricostruire. Le mitigazioni si applicano solo alla fine. Tre regole contano più delle altre. Rimuovere la voce cron prima di terminare il processo, perché il processo la ripristina. Non riavviare la macchina, perché la copia in /proc può essere l'unico binario superstite. Non eseguire composer install come pulizia, perché sovrascrive le date di modifica che documentano cosa è stato toccato.

La ricerca va estesa oltre il crontab: timer systemd anche per utente, at, auto_prepend_file, file PHP in pub/media, chiavi SSH sconosciute. Dentro Magento: account amministrativi non riconosciuti, integrazioni e token API, script iniettati in core_config_data, blocchi CMS modificati. Segue lo svuotamento delle sessioni, che l'impianto leggeva. Vanno poi ruotate la crypt/key in app/etc/env.php, la password del database, tutte le password amministrative, le chiavi API dei fornitori di pagamento e ogni altra credenziale in quel file. Disrex indica anche quando la ricostruzione è preferibile alla pulizia. I casi sono quattro: negozio non sotto controllo di versione; file modificati non spiegabili in vendor/ o app/code/; impianto attivo per giorni; impossibilità di datare l'inizio

della compromissione.

Un ultimo elemento sulla campagna. L'elenco di Disrex, nella revisione più recente, conta 27 indirizzi sorgente distinti su tre negozi e due ondate. La cifra era 26 nella prima versione ed è stata corretta; il README dello stesso repository riporta 28. Tre indirizzi appartengono a infrastrutture di hosting che inviavano in massa; il resto è un insieme di proxy residenziali con due-sei richieste ciascuno. Disrex raccomanda di non bloccare in blocco gli indirizzi residenziali: sono connessioni di consumatori affittate o compromesse, e il blocco costerebbe clienti reali. Bloccare il solo indirizzo citato nell'avviso Sansec avrebbe fermato meno di un quarto del traffico osservato. È un dato di una sola fonte, ma è coerente con l'infrastruttura distribuita tipica delle campagne di web skimming degli ultimi anni.

Riquadro giuridico: cosa scatta quando la compromissione è probabile ma non accertata

Questa sezione ha finalità informativa e non sostituisce il parere di un legale.

Notifica al Garante. L'articolo 33 del GDPR impone al titolare di notificare la violazione all'autorità di controllo senza ingiustificato ritardo e, ove possibile, entro 72 ore da quando ne è venuto a conoscenza. L'obbligo cade se è improbabile che la violazione presenti un rischio per i diritti e le libertà delle persone fisiche. Il nodo, in una situazione come questa, è il momento della "conoscenza". Le Linee guida 9/2022 dell'EDPB (versione 2.0, adottata il 28 marzo 2023) lo definiscono al paragrafo 31. Il titolare è a conoscenza quando ha un ragionevole grado di certezza che un incidente di sicurezza abbia compromesso dati personali. Il paragrafo 34 ammette un breve periodo di indagine iniziale,

durante il quale il titolare non è ancora “a conoscenza”. Il paragrafo 36 precisa però che le verifiche preliminari vanno completate poco dopo il primo allarme, e possono richiedere più tempo solo in casi eccezionali. Il paragrafo 40 aggiunge che chi non agisce tempestivamente e poi scopre la violazione rischia la contestazione di mancata notifica. L'esempio 3 del paragrafo 33 descrive il caso di specie: un titolare rileva una possibile intrusione, controlla i sistemi, conferma la compromissione dei dati e da quel momento è a conoscenza.

Tradotto in pratica. Un esercente che rileva gli indicatori sopra descritti ha superato la soglia, perché l'impianto leggeva le sessioni e aveva accesso a credenziali e chiavi di pagamento; le 72 ore partono da lì. Un esercente che non rileva indicatori, ma non può escludere l'esposizione tra il 4 settembre e l'applicazione delle mitigazioni, si trova nella fase di indagine. Deve avviarla subito, documentarla con date e attività svolte e chiuderla in fretta. L'articolo 33, paragrafo 5, impone di registrare ogni violazione; il paragrafo 125 delle Linee guida chiede di motivare per iscritto anche la decisione di non notificare. L'articolo 33, paragrafo 4, consente la notifica per fasi. Il paragrafo 57 delle Linee guida indica proprio gli incidenti informatici che richiedono analisi forense come il caso tipico in cui il quadro completo manca nelle 72 ore. Il paragrafo 60 ricorda infine che non c'è sanzione per aver notificato un incidente che poi si rivela non essere una violazione.

Comunicazione agli interessati. L'articolo 34 richiede la comunicazione agli interessati quando la violazione è suscettibile di presentare un rischio elevato. La compromissione di un server che gestisce pagamenti rientra quasi sempre in questa categoria. L'esempio ii dell'allegato B delle Linee guida (attacco a un servizio online con esfiltrazione di dati) prevede la notifica all'autorità e, a seconda della gravità, agli interessati. L'esenzione per dati cifrati (paragrafi 76-78) vale solo se la chiave non è stata

compromessa. È da escludere quando la crypt/key di Magento era leggibile dall'utente del sito con cui girava l'impianto. Le stesse Linee guida avvertono che, se la chiave risulta compromessa in un secondo momento, l'obbligo di notifica si riattiva.

Ripartizione delle responsabilità. Nella filiera tipica di un e-commerce italiano l'esercente è titolare del trattamento. L'agenzia che gestisce l'installazione e il fornitore di hosting sono di regola responsabili ai sensi dell'articolo 28. Due conseguenze pratiche. La prima: l'articolo 33, paragrafo 2, obbliga il responsabile a informare il titolare senza ingiustificato ritardo. Il paragrafo 44 delle Linee guida chiarisce che il responsabile non deve prima valutare il rischio; deve solo accertare che la violazione c'è stata e avvisare. Da quel momento il titolare è considerato a conoscenza. Un'agenzia che ha visto gli indicatori sui server dei clienti e non lo ha comunicato ha quindi una responsabilità autonoma. L'esempio vii dell'allegato B (fornitore di hosting che scopre un difetto nel proprio codice) mostra che l'obbligo scatta anche prima di aver accertato lo sfruttamento effettivo.

La seconda: il contratto di servizio è il luogo in cui si decide chi doveva applicare le mitigazioni e in quanto tempo. Molti contratti prevedono l'applicazione delle patch ufficiali entro un certo termine, ma tacciono sul caso in cui una patch ufficiale non esista. Chi decide se applicare una patch di terze parti non revisionata? Chi risponde se quella patch rompe il negozio, o se la mancata applicazione lo espone? Sono domande che i contratti in essere raramente affrontano e che questa vicenda rende urgenti. L'articolo 82, sul diritto al risarcimento, ripartisce la responsabilità civile tra titolare e responsabile in base al rispettivo contributo al danno.

PCI DSS. Per chi è soggetto allo standard, la versione 4.0.1 richiede al requisito 6.3.3 che le patch per le vulnerabilità critiche siano installate entro un mese dal rilascio. Il

requisito presuppone una patch. In sua assenza operano il requisito 6.3.1 (identificazione delle vulnerabilità tramite fonti riconosciute, compresi gli avvisi dei CERT, e loro classificazione per rischio) e i controlli compensativi. I requisiti 6.4.3 e 11.6.1 sono qualificati dallo standard come buone pratiche fino al 31 marzo 2025 e obbligatori da quella data. Il primo impone autorizzazione, integrità e inventario di tutti gli script caricati nelle pagine di pagamento. Il secondo richiede un meccanismo che rilevi le modifiche non autorizzate alle intestazioni HTTP e agli script così come li riceve il browser del cliente, eseguito almeno ogni settimana. Sono esattamente i controlli che intercetterebbero uno skimmer inserito dopo una compromissione via StyleSmuggler. Il requisito 12.10.1 impone infine un piano di risposta agli incidenti, da attivare al primo indicatore.

NIS2. Il singolo negozio online non rientra tra i soggetti del D.Lgs. 138/2024. L'allegato II del decreto include invece i fornitori di mercati online tra i fornitori di servizi digitali. Un fornitore di hosting che gestisce molti e-commerce può rientrare nel perimetro come fornitore di servizi cloud o di data center (allegato I, settore 8, infrastrutture digitali). Un'agenzia che amministra le installazioni Magento dei clienti può rientrarvi come fornitore di servizi gestiti o di servizi di sicurezza gestiti (allegato I, settore 9, gestione dei servizi TIC business-to-business). Restano fermi i criteri dimensionali e la registrazione presso l'ACN. In quel caso l'articolo 25 prevede tre adempimenti per gli incidenti significativi. Una pre-notifica al CSIRT Italia entro 24 ore dalla conoscenza; una notifica entro 72 ore con valutazione iniziale e indicatori di compromissione; una relazione finale entro un mese. Il comma 3 precisa che la notifica non espone chi la effettua a una responsabilità maggiore di quella derivante dall'incidente. I commi 9 e 10 prevedono la comunicazione ai destinatari dei servizi sia degli incidenti sia delle minacce significative, con le misure di mitigazione adottabili. Per un fornitore in perimetro,

StyleSmuggler è una minaccia significativa da comunicare ai clienti anche prima di qualsiasi compromissione accertata.

Cosa aspettarsi dall'8 settembre

La release di sicurezza di Adobe dell'8 settembre è il primo momento in cui il quadro può cambiare. Tre scenari sono possibili. La release include una correzione con relativo CVE. Oppure non la include, e Adobe pubblica un bollettino fuori ciclo nei giorni successivi. Oppure Adobe pubblica prima una soluzione temporanea ufficiale e poi la patch. In ogni caso la finestra successiva va preparata ora.

Chi ha applicato patch non ufficiali deve pianificarne la rimozione prima di installare quella del produttore. La sovrapposizione di modifiche agli stessi file può produrre conflitti o, peggio, l'illusione di aver aggiornato; la patch composer di Disrex prevede un percorso di ritorno esplicito. Chi ha disattivato GraphQL deve avere pronto il piano di riattivazione, con prove funzionali sul pagamento. Chi ha pulito un negozio compromesso deve ricordare che la patch non rimuove una backdoor già installata né invalida credenziali già sottratte. La rotazione dei segreti resta necessaria anche dopo l'aggiornamento.

Resta il punto più scomodo. Un e-commerce compromesso tra il 4 settembre e l'applicazione delle mitigazioni può aver perso dati di pagamento senza che nulla lo segnali, perché l'impianto può operare senza traffico verso indirizzi noti. Per quegli esercenti l'8 settembre non chiude l'incidente. Apre la fase in cui bisogna decidere, con i log alla mano e con un legale al fianco, se e cosa notificare.

<https://www.ictsecuritymagazine.com/notizie/zero-day-magento-stylesmuggler-adobe-commerce/>