Zip Slip: quando un semplice file Zip minaccia la sicurezza



La vulnerabilità Zip Slip, una minaccia tanto sottile quanto devastante che ha colpito giganti tecnologici come Oracle, Amazon, Google, LinkedIn e Twitter.

Un nemico silenzioso nel mondo digitale

Pensate a quante volte al giorno scaricate, aprite o condividete file ZIP. Documenti di lavoro, foto delle vacanze, software, backup: gli archivi compressi sono diventati parte integrante della nostra vita digitale. Ma cosa succederebbe se vi dicessi che dietro quella innocua icona di una cartella compressa si può nascondere una delle minacce informatiche più subdole e devastanti degli ultimi anni?

La storia che sto per raccontarvi inizia nel 2018, quando un gruppo di ricercatori della società di cybersecurity Snyk ha fatto una scoperta che ha letteralmente scosso il mondo della tecnologia. Hanno identificato una vulnerabilità così semplice nel suo funzionamento, eppure così devastante nelle sue conseguenze, da aver colpito migliaia di progetti software utilizzati quotidianamente da miliardi di persone in tutto il mondo.

Questa vulnerabilità ha un nome che suona quasi innocuo: Zip Slip. Ma non lasciatevi ingannare dalla semplicità del nome. Zip Slip ha la capacità di trasformare un normale file ZIP in uno strumento che può permettere a un attaccante di prendere completamente il controllo del vostro computer, rubare i

vostri dati più sensibili o utilizzare il vostro sistema come trampolino di lancio per attacchi ancora più devastanti.

Il meccanismo dell'inganno: come funziona Zip Slip

Per capire come funziona Zip Slip, dobbiamo prima comprendere cosa succede normalmente quando il vostro computer apre un file ZIP. Immaginate il vostro sistema operativo come una grande biblioteca con scaffali ben organizzati. Quando decomprimete un archivio, è come se steste prendendo una scatola di libri e li steste sistemando sullo scaffale giusto.

Normalmente, se la scatola contiene un libro chiamato "Ricette della Nonna", questo finirà nella sezione cucina della vostra biblioteca digitale.

Ma cosa succederebbe se qualcuno riuscisse a etichettare quel libro in modo ingannevole? Invece di chiamarlo semplicemente "Ricette della Nonna", lo etichettasse come "../../Sistema/Password/Ricette della Nonna"? Il vostro bibliotecario digitale, seguendo ciecamente l'etichetta, non metterebbe il libro nella sezione cucina, ma seguirebbe il percorso indicato: uscirebbe dalla sezione attuale, risalirebbe di due livelli nella gerarchia della biblioteca, entrerebbe nella sezione Sistema e poi in quella Password, sistemando il libro (che in realtà contiene codice malevolo) in un luogo dove non dovrebbe mai trovarsi.

Questo è esattamente ciò che accade con Zip Slip. Gli attaccanti creano archivi ZIP che contengono file con nomi speciali, che includono quelle che tecnicamente vengono chiamate "sequenze di attraversamento delle directory". Questi nomi di file contengono simboli come "../" che dicono al sistema operativo: "non mettere questo file dove dovrebbe andare normalmente, ma seguimi mentre navigo fuori dalla cartella sicura verso zone molto più sensibili del sistema".

Una volta che un file malevolo è riuscito a "scappare" dalla sua opportuna destinazione e a finire in una posizione critica

del sistema – come le cartelle che contengono le password degli utenti, i programmi che si avviano automaticamente all'accensione del computer, o i file di configurazione dei servizi più importanti – l'attaccante ha essenzialmente vinto la partita.

La grande rivelazione del 2018: un terremoto nel mondo della tecnologia

Quando i ricercatori di Snyk hanno reso pubblica la loro scoperta il 5 giugno 2018, l'industria tecnologica si è trovata di fronte a una verità sconcertante. Non si trattava di una vulnerabilità che colpiva un singolo software o una specifica azienda. Era un problema sistemico che attraversava praticamente tutto l'ecosistema software moderno.

L'elenco delle aziende e dei progetti colpiti leggeva come un "chi è chi" della tecnologia mondiale. Oracle, il gigante dei *database enterprise* utilizzati da migliaia di aziende in tutto il mondo, doveva fare i conti con software vulnerabile. Amazon, con la sua vasta infrastruttura cloud che supporta una parte significativa di Internet, aveva componenti a rischio. Google, dalle cui applicazioni dipendono miliardi di utenti quotidianamente, aveva prodotti che necessitavano di correzioni urgenti.

Ma non erano solo i colossi tecnologici a essere colpiti. LinkedIn, dove professionisti di tutto il mondo condividono informazioni sensibili sulla loro carriera, aveva vulnerabilità da correggere. Twitter, la piattaforma dove si svolgono dibattiti globali e si condividono notizie in tempo reale, doveva mettere in sicurezza i suoi sistemi. Anche Alibaba, il gigante dell'e-commerce che gestisce transazioni per miliardi di dollari, si è trovata a dover affrontare il problema.

Quello che rendeva la situazione ancora più preoccupante era la diversità dei contesti colpiti. Non si trattava solo di

applicazioni web o software desktop. La vulnerabilità Zip Slip poteva manifestarsi ovunque venissero gestiti archivi compressi: dalle app per smartphone ai sistemi di *backup enterprise*, dai tool di sviluppo software ai sistemi di gestione dei contenuti.

L'aspetto forse più inquietante di tutta la vicenda era quanto fosse stata sottovalutata questa classe di vulnerabilità. Mentre l'industria si concentrava su minacce più "spettacolari" come gli attacchi di phishing elaborati o i ransomware che cifravano interi data center, Zip Slip operava nell'ombra, sfruttando una funzionalità basilare.

I casi che hanno fatto storia: quando la teoria diventa realtà

JFrog Artifactory: il cuore pulsante dello sviluppo software sotto attacco

Nel 2021, tre anni dopo la grande rivelazione iniziale, il mondo della cybersecurity ha ricevuto un'altra scossa quando il ricercatore italiano Egidio Romano ha scoperto una nuova manifestazione di Zip Slip in un luogo particolarmente critico: JFrog Artifactory.

Per chi non è del settore, Artifactory potrebbe sembrare solo un altro software aziendale, ma in realtà è molto di più. È il sistema che migliaia di aziende utilizzano per gestire e distribuire i componenti software che formano le fondamenta delle applicazioni moderne. È come il deposito centrale di una catena di montaggio globale: se viene compromesso, l'effetto si propaga a cascata su tutto ciò che da esso dipende.

La scoperta di Romano è stata particolarmente elegante dal punto di vista tecnico. Aveva identificato che quando Artifactory processava certi tipi di pacchetti software (chiamati "Bower packages"), non validava correttamente i

percorsi dei file contenuti negli archivi. Un attaccante poteva creare un pacchetto malevolo che, una volta processato da Artifactory, avrebbe scritto file in posizioni arbitrarie del server, potenzialmente ottenendo il controllo completo del sistema.

OpenRefine: quando gli strumenti di pulizia hanno bisogno di essere puliti

Nel 2023, un altro caso ha catturato l'attenzione della comunità di cybersecurity, questa volta per le sue implicazioni ironiche. OpenRefine, uno strumento *open-source* utilizzato da *data scientist* e analisti per "pulire" e trasformare *dataset* disordinati, si è rivelato esso stesso bisognoso di una bella pulizia.

La vulnerabilità, catalogata come CVE-2023-37476 con un punteggio di gravità di 7.8 su 10, permetteva agli attaccanti di sfruttare la funzionalità di importazione progetti di OpenRefine per eseguire codice arbitrario sui sistemi delle vittime. L'ironia era palpabile, uno strumento progettato per mettere ordine nei dati poteva essere utilizzato per creare il caos completo nei sistemi che lo ospitavano.

Quello che rendeva questo caso particolarmente preoccupante era il contesto d'uso di OpenRefine. Essendo uno strumento utilizzato principalmente per analizzare dati sensibili – spesso informazioni personali, dati finanziari o intelligence aziendale – una compromissione attraverso Zip Slip poteva avere conseguenze devastanti non solo per il sistema colpito, ma anche per la privacy e la sicurezza dei dati analizzati.

MobSF: il paradosso del guardiano vulnerabile

Il 2024 ha portato con sé quello che molti esperti hanno definito il caso più ironico nella storia delle vulnerabilità Zip Slip. Il Mobile Security Framework (MobSF), uno strumento specializzato nell'identificare vulnerabilità di sicurezza nelle applicazioni mobile, si è rivelato esso stesso

vulnerabile a un attacco Zip Slip di gravità critica, con un punteggio CVSS di 9.8 su 10.

L'ironia della situazione era quasi surreale. Immaginate di scoprire che l'allarme antifurto della vostra casa ha una falla che permette ai ladri di disattivarlo facilmente. MobSF era utilizzato da professionisti della cybersecurity, aziende di sviluppo software e ricercatori di sicurezza per analizzare le app mobile e identificare esattamente il tipo di vulnerabilità di cui esso stesso soffriva.

La vulnerabilità permetteva agli attaccanti di creare file di progetto malevoli che, quando importati in MobSF per l'analisi, potevano sovrascrivere file critici del sistema, incluso il database stesso di MobSF, rendendolo inutilizzabile. Ma le possibilità erano molto più sinistre, un attaccante sufficientemente abile poteva utilizzare questa falla per ottenere l'esecuzione completa di codice sui sistemi utilizzati per l'analisi di sicurezza, potenzialmente compromettendo non solo lo strumento, ma anche tutti i dati sensibili delle app analizzate.

HashiCorp go-slug: l'Infrastruttura cloud nel mirino

Il 2025 si è aperto con quella che molti considerano la scoperta più preoccupante degli ultimi anni nel panorama Zip Slip. Il 21 gennaio, HashiCorp ha annunciato la CVE-2025-0377, una vulnerabilità Zip Slip nella loro libreria *go-slug*, un componente critico dell'ecosistema Terraform utilizzato per gestire l'infrastruttura cloud di migliaia di organizzazioni in tutto il mondo.

Per comprendere la portata di questa scoperta, bisogna capire cosa rappresenta HashiCorp nel panorama tecnologico moderno. Se il *cloud computing* è il sistema nervoso dell'economia digitale contemporanea, HashiCorp fornisce alcuni dei tool più critici per costruire e gestire questo sistema nervoso.

Terraform, il loro prodotto di punta, viene utilizzato da aziende di ogni dimensione per automatizzare la creazione e gestione di infrastrutture cloud complesse.

La libreria *go-slug* colpita dalla vulnerabilità è responsabile di impacchettare e decomprimere i "slugs", archivi compressi che contengono le configurazioni Terraform. Quando un'organizzazione distribuisce la propria infrastruttura cloud attraverso Terraform Enterprise, questi *slugs* viaggiano attraverso la rete, vengono archiviati sui server e poi decompressi per essere processati.

La vulnerabilità permetteva a un attaccante di creare *slug* malevoli che, quando decompressi, potevano scrivere file in posizioni arbitrarie del sistema, potenzialmente compromettendo non solo il server Terraform, ma anche l'intera infrastruttura cloud che da esso dipendeva. Considerando che una singola installazione Terraform può gestire infrastrutture del valore di milioni di dollari, servendo milioni di utenti, le implicazioni di questa vulnerabilità erano terrificanti.

HashiCorp ha reagito rapidamente, rilasciando la versione corretta 0.16.3 della libreria *go-slug*, ma il caso ha servito come un potente promemoria di quanto possa essere delicato l'equilibrio su cui si basa la nostra infrastruttura digitale moderna.

Le conseguenze: un effetto a cascata globale

L'impatto immediato: quando i sistemi crollano

Le conseguenze immediate di un attacco Zip Slip possono essere devastanti e multiformi. A differenza di altri tipi di attacchi informatici che spesso hanno obiettivi specifici, Zip Slip offre agli attaccanti una flessibilità terrificante nella scelta di come e dove colpire.

Uno degli scenari più comuni e devastanti è la sovrascrittura di file di sistema critici. Immaginate un attaccante che riesce a sostituire il file che contiene tutte le password degli utenti di un sistema (il famoso file /etc/passwd nei sistemi Unix), oppure che modifica i file di avvio del sistema operativo per eseguire codice malevolo ogni volta che la macchina si riaccende. In alcuni casi documentati, gli attaccanti hanno utilizzato Zip Slip per installare "cron jobs", compiti automatizzati che il sistema esegue a intervalli regolari, trasformando il computer della vittima in una macchina zombie che esegue silenziosamente le loro istruzioni.

Ma forse ancora più insidioso è l'uso di Zip Slip per compromettere le chiavi SSH, i "pass di accesso" che permettono la connessione remota sicura ai server. Sostituendo o modificando queste chiavi, un attaccante può garantirsi un accesso permanente e difficilmente rilevabile ai sistemi colpiti, creando quello che in gergo viene chiamato un "persistent backdoor".

L'effetto domino nell'industria software

La rivelazione della vulnerabilità Zip Slip ha scatenato quello che può essere descritto solo come un effetto domino globale nell'industria software. Non si è trattato di correggere singole applicazioni o di aggiornare specifici server. È stata necessaria una revisione sistemica di migliaia di progetti software, molti dei quali erano alla base di sistemi critici utilizzati quotidianamente da milioni di persone.

Le aziende hanno dovuto mobilitare team di sviluppatori per esaminare manualmente il codice *legacy*, spesso scritto anni prima quando la consapevolezza di questo tipo di vulnerabilità era limitata. Alcune organizzazioni hanno dovuto sospendere temporaneamente servizi per implementare correzioni d'emergenza. Altre hanno dovuto riscrivere completamente

intere sezioni di codice che gestivano l’estrazione di archivi.

L’impatto è stato particolarmente severo nell’ecosistema Java, dove la mancanza di una libreria standard sicura per la gestione degli archivi aveva portato alla proliferazione di soluzioni artigianali, molte delle quali vulnerabili. Migliaia di sviluppatori avevano copiato e incollato *snippet* di codice da forum come StackOverflow senza rendersi conto che stavano introducendo vulnerabilità critiche nei loro progetti.

Il costo economico della negligenza

Anche se è difficile quantificare con precisione l’impatto economico totale di Zip Slip, le stime parlano di centinaia di milioni di dollari in costi diretti e indiretti. Questi includono non solo i costi immediati per correggere la vulnerabilità, come stipendi per sviluppatori, consulenti di sicurezza, testing aggiuntivo, ma anche i costi meno visibili ma spesso più significativi.

Molte aziende hanno dovuto estendere i cicli di sviluppo dei loro prodotti per implementare controlli di sicurezza aggiuntivi. Alcune hanno perso contratti importanti quando i clienti hanno scoperto che i loro sistemi erano vulnerabili. Altre hanno dovuto aumentare significativamente i loro budget per la cybersecurity e stipulare polizze assicurative più costose.

Ma forse il costo più significativo è stato quello reputazionale. In un’era in cui la fiducia digitale è diventata una valuta critica, le aziende che sono state colpite o che hanno tardato a correggere le vulnerabilità hanno visto danneggiata la loro reputazione presso clienti e partner. Alcune hanno perso posizioni competitive che hanno impiegato anni a ricostruire.

L’evoluzione della difesa: come la tecnologia trasforma la sicurezza informatica

La rivoluzione dell’intelligenza artificiale nella cybersecurity

Una delle risposte più innovative alla sfida posta da Zip Slip è arrivata dall’integrazione dell’intelligenza artificiale nei sistemi di sicurezza. Nel 2024 e 2025, abbiamo assistito a un vero e proprio salto quantico nell’efficacia degli strumenti di rilevazione automatica, con sistemi AI che hanno raggiunto un’accuratezza del 98% nell’identificazione delle vulnerabilità di sicurezza.

Questi sistemi non si limitano a cercare pattern conosciuti di codice vulnerabile, ma utilizzano tecniche di *machine learning* per identificare comportamenti anomali e pattern sospetti che potrebbero indicare tentativi di sfruttamento di Zip Slip. Sono in grado di analizzare in tempo reale il contenuto di archivi compressi, identificando file con nomi sospetti o pattern di *directory traversal* prima che possano causare danni.

Un esempio particolarmente innovativo è Vulnhuntr, sviluppato da Protect AI utilizzando il *large language model* Claude 3.5 Sonnet di Anthropic. Questo strumento è stato specificamente progettato per identificare vulnerabilità zero-day nel codice, incluse nuove varianti di Zip Slip che potrebbero sfuggire ai sistemi di rilevazione tradizionali. In test reali, Vulnhuntr ha già identificato vulnerabilità in progetti GitHub che utilizzano API di grandi aziende tecnologiche, dimostrando l’efficacia dell’approccio basato su AI.

L’approccio della containerizzazione e del

sandboxing

Un’altra strategia che ha guadagnato popolarità è l’uso di tecnologie di containerizzazione e *sandboxing* per isolare i processi di estrazione di archivi. Invece di permettere ai programmi di decomprimere direttamente file sul sistema principale, questi vengono eseguiti in ambienti isolati – “sandbox” digitali – dove eventuali tentativi di scrivere file in posizioni non autorizzate vengono bloccati automaticamente.

Docker e altre tecnologie di containerizzazione sono diventate sempre più popolari proprio per questa capacità di creare ambienti isolati. Quando un’applicazione deve processare un archivio potenzialmente pericoloso, viene eseguita all’interno di un container che ha accesso solo alle risorse strettamente necessarie. Anche se un attacco Zip Slip ha successo, il danno rimane confinato all’interno del container, proteggendo il sistema host.

Lo sviluppo di librerie sicure e standardizzate

Una delle lezioni più importanti apprese dalla crisi Zip Slip è stata la necessità di sviluppare e adottare librerie standardizzate e sicure per la gestione degli archivi. Invece di lasciare che ogni sviluppatore reinventi la ruota, l’industria ha iniziato a convergere verso soluzioni centralizzate che incorporano le migliori pratiche di sicurezza.

Queste librerie implementano automaticamente tutti i controlli necessari per prevenire attacchi di path traversal, liberando gli sviluppatori dalla necessità di implementare e mantenere codice di sicurezza complesso. Molte di queste librerie sono ora sottoposte a audit di sicurezza regolari e a testing automatizzato continuo per garantire che rimangano sicure anche di fronte a new varianti di attacco.

Zip Slip nell’era del cloud e dell’AI: nuove sfide, nuove opportunità

La trasformazione del panorama delle minacce

Con la massiccia migrazione verso il *cloud computing* e l’adozione diffusa di architetture basate su microservizi, la vulnerabilità Zip Slip ha assunto nuove dimensioni e complessità. I sistemi cloud moderni spesso processano migliaia di archivi al minuto, gestendo tutto dai *deployment* di applicazioni ai *backup* automatizzati, dalla distribuzione di contenuti multimediali alla sincronizzazione di dati tra *data center* geograficamente distribuiti.

Questa scala e velocità creano opportunità uniche per gli attaccanti. Un singolo archivio malevolo può essere replicato automaticamente attraverso sistemi di distribuzione globali, potenzialmente compromettendo infrastrutture in continenti diversi in questione di minuti. Allo stesso tempo, la natura effimera di molti servizi cloud – dove server vengono creati e distrutti automaticamente secondo necessità – può rendere difficile rilevare e tracciare attacchi Zip Slip.

L’integrazione con attacchi Multi-Stage

Gli attaccanti moderni raramente utilizzano Zip Slip come attacco isolato. Invece, lo integrano in quello che vengono chiamate “kill chain” o catene di attacco *multi-stage*. Un attacco tipico potrebbe iniziare con una campagna di phishing che distribuisce archivi compressi malevoli. Una volta che Zip Slip permette l’accesso iniziale al sistema, gli attaccanti utilizzano questo punto d’appoggio per muoversi lateralmente nella rete, escalare privilegi, e infine raggiungere i loro obiettivi principali.

Questa evoluzione ha reso la difesa ancora più complessa,

perché non è sufficiente proteggere contro Zip Slip in isolamento. Le organizzazioni devono pensare in termini di difesa in profondità, implementando controlli a multiple livelli che possano rilevare e bloccare attacchi anche quando uno dei livelli viene superato.

La preparazione per l'era quantistica

Guardando al futuro, c'è una dimensione ancora più preoccupante da considerare. Con l'avvicinarsi dell'era dei computer quantistici, che promettono di rendere obsoleti molti degli algoritmi crittografici attuali, vulnerabilità come Zip Slip potrebbero diventare ancora più pericolose.

Gli esperti di sicurezza hanno iniziato a parlare di attacchi "*harvest now, decrypt later*" – dove gli attaccanti raccolgono oggi dati crittografati con l'intenzione di decifrarli in futuro quando i computer quantistici saranno disponibili. In questo contesto, Zip Slip potrebbe essere utilizzato non solo per compromissioni immediate, ma anche per installare meccanismi di raccolta dati dormienti che potrebbero rimanere nascosti per anni, raccogliendo silenziosamente informazioni che diventeranno vulnerabili nell'era quantistica.

Lezioni apprese e raccomandazioni per il futuro

Per le organizzazioni: la sicurezza come processo continuo

La storia di Zip Slip insegna alle organizzazioni che la sicurezza non può essere vista come un progetto con un inizio e una fine, ma deve essere integrata come un processo continuo in tutte le operazioni IT. Questo significa implementare quello che viene chiamato un "Security Development Lifecycle" (SDLC), dove considerazioni di sicurezza sono integrate in ogni fase dello sviluppo software.

Le organizzazioni più mature hanno iniziato a implementare quello che viene chiamato “shift-left security”, spostando i controlli di sicurezza il più a sinistra possibile nel ciclo di sviluppo. Invece di testare la sicurezza solo prima del *deployment*, questi controlli vengono integrati negli IDE degli sviluppatori, nei sistemi di controllo versione, nelle *pipeline* di integrazione continua, e in ogni altro punto dove il codice viene creato o modificato.

Per gli sviluppatori: l’Importanza della formazione continua

Per gli sviluppatori, Zip Slip rappresenta un promemoria potente dell’importanza di rimanere aggiornati sulle minacce di sicurezza e le migliori pratiche. Non è sufficiente sapere come scrivere codice funzionale; nel mondo moderno, ogni sviluppatore deve anche essere un mini-esperto di sicurezza, capace di riconoscere e prevenire vulnerabilità comuni.

Questo richiede un investimento continuo in formazione e aggiornamento. Molte aziende hanno iniziato a richiedere certificazioni di sicurezza per i loro sviluppatori, mentre altre hanno implementato programmi di formazione interni che coprono regolarmente le minacce emergenti e le tecniche di difesa.

Per l’industria: la necessità di collaborazione

A livello industriale, Zip Slip ha evidenziato l’importanza della collaborazione nella cybersecurity. Le minacce moderne sono troppo complesse e sofisticate per essere affrontate da singole organizzazioni operando in isolamento. La condivisione di informazioni sulle minacce, la collaborazione nello sviluppo di standard di sicurezza, e l’investimento collettivo in ricerca e sviluppo di nuove tecnologie di difesa sono diventati non solo vantaggiosi, ma essenziali per la sopravvivenza.

Iniziative come il repository GitHub mantenuto da Snyk, che

documenta tutte le librerie e i progetti vulnerabili a Zip Slip, rappresentano esempi eccellenti di come la condivisione aperta di informazioni possa beneficiare l'intera comunità. Questo tipo di trasparenza e collaborazione deve essere espanso e istituzionalizzato per affrontare efficacemente le minacce future.

Riflessioni finali: il futuro della sicurezza in un mondo interconnesso

Mentre guardiamo al futuro, la storia di Zip Slip ci offre lezioni preziose che vanno ben oltre la specifica vulnerabilità tecnica. Ci ricorda che in un mondo sempre più interconnesso e digitale, la sicurezza non è un lusso o un'aggiunta opzionale, ma una necessità fondamentale che deve essere integrata nel DNA di ogni sistema tecnologico.

La persistenza di questa vulnerabilità attraverso gli anni – dalla sua scoperta iniziale nel 2018 fino alle manifestazioni più recenti del 2025 – dimostra che la sicurezza informatica è una sfida in continua evoluzione. Non esistono soluzioni definitive o stati di sicurezza permanenti. Ogni nuovo software, ogni nuova tecnologia, ogni nuovo modo di utilizzare strumenti esistenti può introdurre nuove vulnerabilità o rivelare nuovi modi di sfruttare debolezze già conosciute.

Ma la storia di Zip Slip è anche una storia di resilienza e innovazione. L'industria ha risposto alla sfida con creatività e determinazione, sviluppando nuovi strumenti, nuove metodologie, e nuovi approcci alla sicurezza. L'integrazione dell'intelligenza artificiale nella cybersecurity, lo sviluppo di tecnologie di containerizzazione più sofisticate, e l'evoluzione verso architetture di sicurezza più robuste sono tutte conseguenze positive della lezione imparata da Zip Slip.

Mentre ci muoviamo verso un futuro che includerà computer quantistici, intelligenza artificiale ancora più avanzata, e

livelli di interconnessione digitale che oggi possiamo solo immaginare, le lezioni fondamentali di Zip Slip rimangono valide: la semplicità può essere devastante, la vigilanza deve essere costante, e la sicurezza è responsabilità di tutti.

Ogni volta che scarichiamo un file ZIP, ogni volta che un'applicazione processa un archivio, ogni volta che un sistema automatizzato gestisce contenuti compressi, c'è un momento di potenziale vulnerabilità. La differenza tra sicurezza e compromissione spesso risiede in dettagli apparentemente insignificanti, una validazione di percorso non implementata, un controllo di sicurezza saltato per risparmiare tempo, una libreria non aggiornata perché "funzionava già bene così".

Zip Slip ci insegna che nella cybersecurity, come nella vita, spesso sono le minacce che non vediamo arrivare quelle che possono farci più male. Ma ci insegna anche che con la giusta attenzione, le giuste conoscenze, e il giusto impegno collettivo, anche le minacce più subdole possono essere identificate, comprese, e sconfitte.

La prossima volta che vedrete l'icona di un file ZIP, ricordatevi di questa storia. Quel piccolo simbolo innocuo rappresenta non solo la convenienza della compressione digitale, ma anche la complessità e la responsabilità che vengono con la vita nel mondo digitale moderno. E forse, con questa consapevolezza, saremo tutti un po' più sicuri.

Fonti:

- Snyk Security Team. "Zip Slip Vulnerability." *Snyk Vulnerability Database*, 2018. [Online]. Available: https://security.snyk.io/research/zip-slip-vulnerability. [Accessed: May 2025].
- Snyk Security Team. "Zip Slip Vulnerability – Arbitrary file write through archive extraction." *GitHub Repository*, 2018. [Online]. Available:

https://github.com/snyk/zip-slip-vulnerability.
- MITRE Corporation. “CWE-22: Improper Limitation of a Pathname to a Restricted Directory (‘Path Traversal’).” *Common Weakness Enumeration*, 2025. [Online]. Available: https://cwe.mitre.org/data/definitions/22.html.
- National Institute of Standards and Technology. “National Vulnerability Database.” *NIST*, U.S. Department of Commerce, 2025. [Online]. Available: https://nvd.nist.gov/.
- HashiCorp Inc. “HCSEC-2025-01 – HashiCorp go-slug Vulnerable to Zip Slip Attack.” *HashiCorp Security Advisory*, Jan. 21, 2025. [Online]. Available: https://discuss.hashicorp.com/t/hcsec-2025-01-hashicorp-go-slug-vulnerable-to-zip-slip-attack/72719.
- GitHub Advisory Database. “HashiCorp go-slug Vulnerable to Zip Slip Attack – CVE-2025-0377.” *GitHub Security Advisories*, Jan. 28, 2025. [Online]. Available: https://github.com/advisories/GHSA-wpfp-cm49-9m9q.
- SecurityOnline.info. “CVE-2024-43399: Critical Zip Slip Vulnerability Discovered in Mobile Security Framework (MobSF).” *Security Online*, Aug. 26, 2024. [Online]. Available: https://securityonline.info/cve-2024-43399-critical-zip-slip-vulnerability-discovered-in-mobile-security-framework-mobsf/.
- Guru Baran. “New Zip Slip vulnerability Let Attackers Execute Arbitrary Code Via Path Traversal.” *Cybersecurity News*, Jun. 25, 2024. [Online]. Available: https://cybersecuritynews.com/new-zip-slip-vulnerability/.
- The Hacker News. “OpenRefine’s Zip Slip Vulnerability Could Let Attackers Execute Malicious Code.” Oct. 2, 2023. [Online]. Available: https://thehackernews.com/2023/10/openrefines-zip-slip-vulnerability.html.
- OWASP Foundation. “Path Traversal.” *OWASP Community Pages*, 2025. [Online]. Available:

https://owasp.org/www-community/attacks/Path_Traversal.
- OWASP Foundation. “16.2 Safe from path traversal.” *OWASP Application Security Verification Standard v3.0.0*, 2025. [Online]. Available: https://owasp-aasvs.readthedocs.io/en/latest/requirement-16.2.html.
- Google LLC. “Arbitrary file access during archive extraction (Zip Slip) — CodeQL query help.” *GitHub CodeQL*, 2025. [Online]. Available: https://codeql.github.com/codeql-query-help/go/go-zipslip/.
- Cybersecurity and Infrastructure Security Agency. “Pilot for Artificial Intelligence Enabled Vulnerability Detection.” *CISA Resources*, 2024. [Online]. Available: https://www.cisa.gov/resources-tools/resources/pilot-artificial-intelligence-enabled-vulnerability-detection.
- Akshaya Asokan. “Researchers Debut AI Tool That Helps Detect Zero-Days.” *Bank Info Security*, Oct. 21, 2024. [Online]. Available: https://www.bankinfosecurity.com/researchers-debut-ai-tool-that-helps-detect-zero-days-a-26575.
- AnyAPI Team. “AI Cybersecurity in 2025: From Threat Detection to Automated Response.” *AnyAPI Blog*, Feb. 12, 2025. [Online]. Available: https://anyapi.io/blog/AI-Cybersecurity-in-2025-From-Threat-Detection-to-Automated-Response.
- The Hacker News. “159 CVEs Exploited in Q1 2025 — 28.3% Within 24 Hours of Disclosure.” Apr. 24, 2025. [Online]. Available: https://thehackernews.com/2025/04/159-cves-exploited-in-q1-2025-283.html.
- Google LLC. “Zip Path Traversal.” *Android Developers — Privacy and Security*, 2023. [Online]. Available: https://developer.android.com/privacy-and-security/risks/zip-path-traversal.
- Go Security Team. “Vulnerability Reports.” *Go Packages*, 2025. [Online]. Available: https://pkg.go.dev/vuln/list.

- The Hacker News. “‘Zip Slip’ Vulnerability Affects Thousands of Projects Across Many Ecosystems.” Jun. 5, 2018. [Online]. Available: https://thehackernews.com/2018/06/zipslip-vulnerability.html.
- Catalin Cimpanu. “Zip Slip Vulnerability Affects Thousands of Projects Across Multiple Ecosystems.” *Bleeping Computer*, Jul. 16, 2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/zip-slip-vulnerability-affects-thousands-of-projects-across-multiple-ecosystems/.
- Help Net Security. “Zip Slip vulnerability affects thousands of projects.” Jun. 7, 2018. [Online]. Available: https://www.helpnetsecurity.com/2018/06/05/zip-slip-vulnerability/.
- OX Security. “A Guide to Protect You Against the Zip Slip Attack.” Sep. 30, 2024. [Online]. Available: https://www.ox.security/protecting-against-the-zip-slip-vulnerability-attack/.
- INE Security. “The Zip Slip Vulnerability: Zip Files Slipping under Your Nose!” *INE Blog*, 2024. [Online]. Available: https://ine.com/blog/the-zip-slip-vulnerability.
- GBHackers. “Zip Slip Vulnerability Let Attacker Import Malicious Code and Execute Arbitrary Code.” Sep. 2, 2024. [Online]. Available: https://gbhackers.com/zip-slip-vulnerability/.
- CVE Program. “CVE – Common Vulnerabilities and Exposures.” *MITRE Corporation*, sponsored by CISA, 2025. [Online]. Available: https://cve.mitre.org/.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/zip-slip-vulnerability/