

ESPLORAZIONE DEI CVE SHOPIFY

ChatGPT, potresti fornirmi una lista dei CVE relativi a Shopify? Vorrei anche informazioni dettagliate su alcuni di essi, inclusi i dettagli delle vulnerabilità e le soluzioni consigliate.

Ecco una lista di vulnerabilità relative a Shopify (CVE) insieme a informazioni dettagliate su alcune delle più significative:

1. **CVE-2020-8176:**

Una vulnerabilità di **Cross-Site Scripting (XSS)** nella libreria `koa-shopify-auth` (versioni 3.1.61 - 3.1.62). Questa vulnerabilità consente a un attaccante di iniettare payload JavaScript nel parametro `shop` sull'endpoint `/shopify/auth/enable_cookies`. Ciò può portare all'esecuzione non autorizzata di script nel browser della vittima. La soluzione consigliata è aggiornare a una versione corretta.

2. **CVE-2022-29230:**

Un'altra vulnerabilità XSS che interessa **Shopify Hydrogen** (versioni 0.10.0 a 0.18.0). Hydrogen è un framework utilizzato per creare storefront dinamici basati su Shopify. In questo caso, una gestione impropria dei dati utente consente l'esecuzione arbitraria di script su siti web costruiti con Hydrogen. La soluzione è aggiornare alla versione 0.19.0 o successiva.

3. **CVE-2022-44634:**

Una vulnerabilità di **lettura arbitraria di file** nel plugin "S2W - Import Shopify to WooCommerce" per WordPress (versioni $\leq 1.1.12$). Questa vulnerabilità consente a un attaccante autenticato (con privilegi di amministratore) di leggere file arbitrari dal server, potenzialmente esponendo dati sensibili. La vulnerabilità è stata risolta nelle versioni successive.

4. **CVE-2024-45036:**

Questa vulnerabilità riguarda **Tophat**, un ambiente di test per applicazioni mobili utilizzato con Shopify. Un problema di controllo degli accessi può esporre il `TOPHAT_APP_TOKEN`, permettendo agli attaccanti di accedere a artefatti interni di build. L'aggiornamento alla versione 1.10.0 risolve il problema.

5. **CVE-2018-3740:**

Una vulnerabilità nella gemma **Sanitize** per Ruby, utilizzata da Shopify. Questo difetto consente a un frammento HTML appositamente costruito di bypassare la sanitizzazione e iniettare attributi non autorizzati negli elementi consentiti. Riguarda i negozi Shopify che utilizzano versioni vulnerabili di questa libreria.

Raccomandazioni generali:

- ⑩ **Aggiornamenti rapidi:** Assicurarsi che tutte le librerie e i plugin di Shopify siano aggiornati alle versioni più recenti per correggere eventuali vulnerabilità.
- ⑩ **Abilitare header di sicurezza:** Implementare politiche di sicurezza dei contenuti (**CSP**) può aiutare a mitigare i rischi associati agli attacchi XSS.
- ⑩ **Usare autenticazione forte:** Limitare l'accesso amministrativo agli utenti necessari e considerare l'uso dell'**autenticazione a più fattori (MFA)** per prevenire accessi non autorizzati.

Per un elenco completo dei CVE di Shopify e i relativi dettagli, puoi visitare siti di monitoraggio come Vulmon, OpenCVE o il database CVE di Mitre.