Doppia falla nel plugin MAGMI per Magento

Set 02, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Due vulnerabilità permetterebbero di prendere il controllo di un sito e per una delle due non c'è ancora la patch.

Allarme rosso per chi utilizza la piattaforma **Magento** (il più diffuso Content Management System dedicato all'e-commerce – ndr) con il plugin **MAGMI**.

Come riporta in un post il Security Response Team di **Tenable**, il diffusissimo plugin è viziato da una serie di vulnerabilità che consentirebbero a un pirata informatico di eseguire codice in remoto, aprendo quindi la strada alla compromissione del sistema.

MAGMI è un acronimo che sta per *Magento Mass Import* ed è un database scritto in PHP creato per la gestione dei cataloghi in Magento. **Stando alle ricerche effettuate dagli analisti, verrebbe utilizzato da almeno 1.500 siti di e-commerce nel mondo**.

La prima vulnerabilità segnalata dai ricercatori (CVE-2020-5777) consentirebbe di aggirare il sistema di autenticazione nelle installazioni Magento che utilizzano MAGMI fino alla versione 0.7.23. La nuova versione del plugin (0.7.24) corregge la falla di sicurezza.

Nessuna patch, almeno per il momento, per la seconda vulnerabilità (CVE-2020-5776) individuata da Tenable. Il bug in questione riguarda una funzionalità di uno specifico file (*/index.php/newsletter/subscriber/new/*) che consentirebbe di "dirottare" l'accesso a Magento.

Per mettere a segno l'attacco, un pirata informatico dovrebbe riuscire a indurre l'amministratore del sito ad aprire un link malevolo mentre è autenticato nel CMS.

Insomma: la vulnerabilità non può essere sfruttata per portare attacchi diretti ai siti Internet di e-commerce che utilizzano il plugin, ma richiede l'uso di tecniche di phishing o altri stratagemmi di ingegneria sociale.

I ricercatori, in ogni caso, suggeriscono di disattivare (o disinstallare) il plugin fino a quando non sarà disponibile un nuovo aggiornamento in grado di correggere la falla di

sicurezza.

Considerato che Magento viene utilizzato per l’e-commerce e che la presenza di sistemi di pagamento online rappresentano una formidabile attrattiva per i pirati informatici, il suggerimento ha una sua logica.

Condividi l’articolo

Hacker al soldo del governo iraniano vendono online accessi ai server

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/09/02/doppia-falla-nel-plugin-magmi-per-magento/?utm_source=rss&utm_medium=rss&utm_campaign=doppia-falla-nel-plugin-magmi-per-magento