Gabriele Di giampietro **Data 24/11/2022**

Report per il tecnico / 3 Vulnerabilità livello High su Metasploitable

Informazioni Host:

Netbios Name: METASPLOITABLE IP: 192.168.50.101

MAC Address: 08:00:27:D9:D6:ED

OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

70728 - Apache PHP-CGI Remote Code Execution

- Descrizione:

L'installazione di PHP sul server Web remoto contiene un difetto che potrebbe consentire a un utente malintenzionato in remoto di passare argomenti della riga di comando come parte di una stringa di query al programma PHP-CGI. Questo potrebbe essere abusato per eseguire il codice in modo arbitrario, rivelare il codice sorgente PHP, causare un arresto anomalo del sistema, ecc.

- Soluzione:

Aggiornare a PHP 5.3.13 / 5.4.3 o successivo.

- Risk Factor: High (Alto)
- Plugin Output: tcp/80/www

19704 - TWiki 'rev' Parameter Arbitrary Command Execution

- Descrizione:

La versione di TWiki in esecuzione sull'host remoto consente a un utente malintenzionato di manipolare l'input al parametro 'rev' per eseguire comandi shell arbitrari sull'host remoto soggetto ai privilegi dell'id utente del server web.

- Soluzione:

Applicare l'hotfix (aggiornamento rapido specifico) appropriato a cui si fa riferimento nell'avviso del fornitore.

- Risk Factor: High (Alto)
- Plugin Output: tcp/80/www

36171 - phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)

- Descrizione:

Lo script di installazione incluso con la versione di phpMyAdmin installata sull'host remoto non depura correttamente l'input fornito dall'utente prima di utilizzarlo per generare un file di configurazione per l'applicazione.

Questa versione di phpMyAdmin è interessata dalle seguenti vulnerabilità:

- Lo script di installazione inserisce il nome del server dettagliato non codificando in un commento in stile C durante la generazione del file di configurazione.

- Un utente malintenzionato può salvare dati arbitrariamente nel file di configurazione generato, modificando il valore del parametro "textconfig" durante una richiesta POST a config.php.

Un utente malintenzionato da remoto non autenticato può sfruttare questi problemi per eseguire codice PHP arbitrari.

- Soluzione:

Aggiornare a phpMyAdmin 3.1.3.2. In alternativa, applica le patch a cui si fa riferimento nell'avviso del progetto.

- Risk Factor: High (Alto)
- Plugin Output: tcp/80/www