Rischio: ALTO 8.8 70728 Apache PHP-CGI Remote Code Execution

Sinossi:
Il server web remoto contiene una versione di PHP che consente l'esecuzione di codice arbitrario.

Descrizione:
L'installazione di PHP sul server web remoto contiene un difetto che potrebbe consentire un controllo remoto, utente malintenzionato per passare argomenti della riga di comando come parte di una stringa di query al programma PHP-CGI. Questo potrebbe essere abusato per eseguire codice arbitrario, rivelare codice sorgente PHP, causare crash al sistema, ecc.

Soluzione:
Aggiornare a PHP 5.3.13 / 5.4.3 o successivo.

Rischio: ALTO 8.8 19704 Twiki ‘rev’ Parameter Arbitrary Command Execution

Sinossi:
Il server Web remoto ospita un'applicazione CGI interessata da un comando arbitrario vulnerabilità di esecuzione.

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

Soluzione:
Applicare l'aggiornamento rapido appropriato a cui si fa riferimento nell'avviso del fornitore. (https://twiki.org/cgi-bin/view/Codev/SecurityAlertExecuteCommandsWithRev)

Rischio: ALTO 8.6 136769 ISC BIND Service Downgrade / Reflected DoS

Sinossi:
Il server dei nomi remoto è interessato dalle vulnerabilità di downgrade del servizio / DoS riflesso.

Descrizione:
Secondo la sua versione auto-riportata, l'istanza di ISC BIND 9 in esecuzione sul nome remoto il server è interessato dal downgrade delle prestazioni e dalle vulnerabilità DoS riflesse. Questo è dovuto a BIND DNS non limita a sufficienza il numero di recuperi che possono essere eseguiti durante elaborazione di una risposta di riferimento. Un utente malintenzionato remoto non autenticato può sfruttarlo per causare il degrado del servizio di server ricorsivo o per utilizzare il server interessato come riflettore in un Reflection attack.

Soluzione:
Aggiornamento alla versione ISC BIND a cui si fa riferimento nell'avviso del fornitore. (https://kb.isc.org/docs/cve-2020-8616)