REPORT CRITICITA’

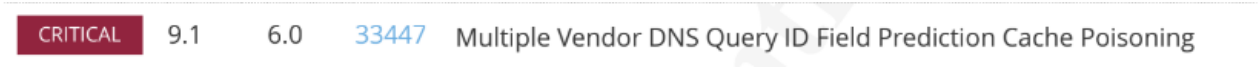
Rischi:

Questa vulnerabilità consente a un attaccante remoto di eseguire un attacco di injection.

Gli attaccanti possono sfruttare questa vulnerabilità per eseguire varie azioni dannose, come la lettura o la modifica di file sensibili sul server o l'esecuzione di codice consentendo loro di prendere il controllo completo del sistema.

Soluzioni:

Applicare le patch di sicurezza fornite dagli sviluppatori, limitare gli accessi



Rischi:

La vulnerabilità potrebbe portare alla cache poisoning, una tecnica attraverso la quale un attaccante inserisce dati malevoli nella cache DNS di un server, in modo che le future richieste di risoluzione DNS possano essere reindirizzate verso risorse dannose controllate dall'attaccante anziché verso i veri server legittimi.

Soluzioni:

Randomizzare gli ID nelle query DNS, applicazione di patch per migliorare la sicurezza, l'uso di DNSSEC (Domain Name System Security Extensions) per la firma digitale.

Rischi:

Attacchi di Dos, l’attaccante può ridurre i livelli di sicurezza del serbizio BIND

Soluzioni:

Applicare le patch BIND, monitorare l’infrastruttura, segmentare la rete.