Offene MySQL-Datenbanken mit Standard-Passwort

CERT-Bund hat von CERT-EE Informationen zu Systemen in Deutschland erhalten, auf denen auf Port 3306/tcp ein MySQL-Datenbankserver läuft, welcher offen aus dem Internet erreichbar ist und eine Anmeldung als Datenbankadministrator mit dem Benutzer 'root' und einem Standard-Passwort ('root', 'admin' oder 'password') erlaubt. Angreifer können dies ausnutzen, um vollständigen Zugriff auf den Datenbankserver zu erlangen und beliebige Daten auszuspähen, zu löschen oder zu manipulieren. Ja nach Konfiguration können auch beliebige Shell-Kommandos auf dem System darüber ausgeführt werden.

Nachfolgend senden wir Ihnen Informationen zu betroffenen Systemen in Ihrem Netzbereich. Leider liegen uns keine exakten Zeitstempel vor, wann die offenen Datenbanken identifiziert wurden.

Wir möchten Sie bitten, den Sachverhalt zu prüfen und entsprechende Maßnahmen zur Absicherung der Systeme einzuleiten bzw. Ihre Kunden entsprechend zu informieren.

Quelle: https://support.belwue.de/sicherheit/sicherheitswarnungen/offene-mysql-datenbanken-mit-standard-passwort/