Offene LDAP-Server

Das Lightweight Directory Access Protocol (LDAP) ist ein Netzwerkprotokoll zur Abfrage und Verwaltung von Informationen verteilter Verzeichnisdienste.

In den letzten Monaten wurden Systeme, welche LDAP-Anfragen aus dem Internet beantworten, zunehmend zur Durchführung von DDoS-Reflection-Angriffen gegen IT-Systeme Dritter missbraucht.

Nachfolgend senden wir Ihnen eine Liste betroffener Systeme in Ihrem Netzbereich. Der Zeitstempel (Zeitzone UTC) gibt an, wann der offene LDAP-Server identifiziert wurde.

Wir möchten Sie bitten, den Sachverhalt zu prüfen und Maßnahmen zur Absicherung der LDAP-Dienste auf den betroffenen Systemen zu ergreifen bzw. Ihre Kunden entsprechend zu informieren.

Falls Sie kürzlich bereits Gegenmaßnahmen getroffen haben und diese Benachrichtigung erneut erhalten, beachten Sie bitten den angegebenen Zeitstempel. Wurde die Gegenmaßnahme erfolgreich umgesetzt, sollten Sie keine Benachrichtigung mit einem Zeitstempel nach der Umsetzung mehr erhalten.

Quelle: https://support.belwue.de/sicherheit/sicherheitswarnungen/offene-ldap-server/