Offene NetBIOS-Namensdienste

NetBIOS ist eine Programmierschnittstelle zur Kommunikation zwischen Programmen über ein lokales Netzwerk.

NetBIOS over TCP/IP ist ein Netzwerkprotokoll, das es ermöglicht, auf der Programmierschnittstelle NetBIOS aufbauende Programme über das Netzwerkprotokoll TCP/IP zu verwenden.

In den letzten Monaten wurden Systeme, welche Anfragen an NetBIOS-Namensdienste aus dem Internet beantworten, zunehmend zur Durchführung von DDoS-Reflection-Angriffen gegen IT-Systeme Dritter missbraucht. Der NetBIOS-Namensdienst verwendet Port 137/udp.

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

Wir möchten Sie bitten, den Sachverhalt zu prüfen und Maßnahmen zur Absicherung der NetBIOS-Namensdienste 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.

Weitere Informationen

For more information on this report go to:

- Shadowserver: Open NetBIOS Report [1]
- Shadowserver: Open NetBIOS Scanning Project [2]

Links

[1] https://www.shadowserver.org/what-we-do/network-reporting/open-netbios-report/
[2] https://scan.shadowserver.org/netbios/

Quelle: https://support.belwue.de/sicherheit/sicherheitswarnungen/offene-netbios-namensdienste/