Multicast DNS (mDNS)

Multicast DNS (mDNS) dient der Auflösung von Hostnamen zu IP-Adressen in lokalen Netzwerken, welche nicht über einen DNS-Server verfügen. Implementierungen von mDNS sind z. B. Apple "Bonjour" oder "Avahi" bzw. "nss-mdns" unter Linux/BSD. mDNS verwendet Port 5353/udp [1].

Neben der Preisgabe von Informationen über das System/Netzwerk können offen aus dem Internet erreichbare mDNS-Dienste für DDoS-Reflection/Amplification-Angriffe gegen Dritte missbraucht werden [2] [3].

Im Rahmen des Shadowserver "Open mDNS Scanning Projects" werden Systeme identifiziert, welche mDNS-Anfragen aus dem Internet beantworten und dadurch für DDoS-Angriffe missbraucht werden können, sofern keine anderen Gegenmaßnahmen implementiert wurden.

CERT-Bund erhält von Shadowserver die Testergebnisse für IP-Adressen in Deutschland, um betroffene Systembetreiber benachrichtigen zu können. Weitere Informationen zu den von Shadowserver durchgeführten Tests finden Sie unter [4].

Nachfolgend senden wir Ihnen eine Liste betroffener Systeme in Ihrem Netzbereich. Der Zeitstempel gibt an, wann das System geprüft wurde und mDNS-Anfragen aus dem Internet beantwortet hat. Wir möchten Sie bitten, den Sachverhalt zu prüfen und Maßnahmen zur Absicherung der mDNS-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.

Referenzen

[1] Wikipedia: Multicast DNS [1]
[2] US-CERT: UDP-based Amplification Attacks [2]
[3] US-CERT: Multicast DNS (mDNS) implementations may respond to unicast queries originating outside the local link [3]
[4] Shadowserver: Open mDNS Scanning Project [4]

Links

[1] https://en.wikipedia.org/wiki/Multicast_DNS
[2] https://www.us-cert.gov/ncas/alerts/TA14-017A
[3] http://www.kb.cert.org/vuls/id/550620
[4] https://scan.shadowserver.org/mdns/

Quelle: https://support.belwue.de/sicherheit/sicherheitswarnungen/mdns/