NTP Monlist

Im Rahmen des Shadowserver "Open NTP Monitor Scanning Projects" werden NTP-Server identifiziert, welche aktuell noch eine Anfrage mittels des "monlist"-Kommandos beantworten. Diese NTP-Server können potenziell für DDoS-Angriffe mittels NTP-Amplification missbraucht werden, sofern keine anderen Gegenmaßnahmen implementiert wurden.

Referenzen

[1] BSI: CERT-Bund-Reports: NTP servers with 'monlist' enabled [1]
[2] BSI: Maßnahmen gegen Reflection Angriffe [2]
[3] CERT.org: NTP can be abused to amplify denial-of-service attack traffic [3]
[4] US-CERT: NTP Amplification Attacks Using CVE-2013-5211 [4]
[5] NTP.org Security Notice [5]

Links

[1] https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Reaktion/CERT-Bund/CERT-Bund-Reports/HowTo/NTP-Server-Monlist/NTP-Server-Monlist.html
[2] https://support.belwue.de/sicherheit/sicherheitswarnungen/ntp-monlist_BSI-CS_096.pdf
[3] http://www.kb.cert.org/vuls/id/348126
[4] https://www.us-cert.gov/ncas/alerts/TA14-013A
[5] http://support.ntp.org/bin/view/Main/SecurityNotice

Quelle: https://support.belwue.de/sicherheit/sicherheitswarnungen/ntp-monlist/