

Tag Vuln.ntpd_monlist

[[Kurzinfo](#)] [[Treffsicherheit](#)] [[Beschreibung](#)] [[Gegenmaßnahmen](#)] [[Erfahrungen](#)]

Kurzinfo

Ntp-Server, die den monlist-Befehl öffentlich erlauben, können für DoS-Angriffe missbraucht werden.

Treffsicherheit

Im Prinzip hoch, jedoch wird ein Rate-Limit vom Test nicht erkannt.

Beschreibung

Die Schwachstelle beruht auf folgenden Faktoren:

- ntp kommuniziert mittels UDP und die UDP source IP kann leicht verändert werden auf die IP des anzugreifenden Zieles
- der monlist command liefert eine Liste mit den letzten 600 anfragenden Clients zurück
- die Antwort kann bis zu 200 mal größer sein als die Anfrage (=Amplifizierung)
- der monlist command ist bis NTP server Version 4.2.7 per default aktiviert (ab Version 4.2.7 aber per default geschlossen)

Der Zugehörige Angriff ist unter [Amplified UDP reflection attack](#) ausführlich beschrieben.

Überprüfen ob der eigene ntp-Server für diese Attacke verwundbar ist, kann man mit folgendem Kommando:

```
ntpd -n -c monlist IP-Adresse
```

Erscheint als Antwort eine Adressliste, ist der ntp-Server für diesen Angriff verwundbar. Der Switch "monlist" dient eigentlich nur zu Monitoring/Statistik- Zwecken. Es werden dabei die Adressen der anfragenden Server zurückgegeben. Daher ist es unbedenklich, wenn dieser Switch/Kommando in der /etc/ntp.conf deaktiviert wird mit:

```
disable monitor
```

Für Teilnehmer, die keinen eigenen ntp (Timeserver) betreiben, bietet das AConet den ts1.aco.net und ts2.aco.net an.

Gegenmaßnahmen

Da es sich meist um eine Fehlkonfiguration handelt, haben sich folgende Schritte bewährt:

- Prüfen ob der NTP SERVER Dienst auf dem Gerät wirklich benötigt wird und diesen eventuell deaktivieren (der NTP CLIENT kann aktiviert bleiben).
- **Aktualisieren des NTP Server auf die Version 4.2.7 oder höher.** Bei diesen Versionen ist der monlist command per default abgeschaltet.
- Zugriff auf den NTP Server Dienst des Geräts auf das lokale Netz beschränken.
- Monlist command manuell in der Konfiguration abschalten.

Sehr gute Hilfestellung bei der Ergreifung der individuell besten Maßnahmen finden sie auf [ntp.org - ntpd access restrictions](#).

Links

US-CERT Alert (TA14-013A) NTP Amplification Attacks Using CVE-2013-5211
<https://www.us-cert.gov/ncas/alerts/TA14-013A>

Kommt Zeit, kommt – DDoS-Angriff (Artikel auf Heise-Security)[AC](#)
<http://www.heise.de/-2087846.html>

Secure NTP Template. Konfigurations-Empfehlungen von Team Cymru.
<https://www.team-cymru.com/secure-ntp-template.html>

ACOnet-Timeserver
<http://www.aco.net/timeserver.html?&L=0>

Erfahrungen

Derzeit keine vermerkt.