Date: 2/14/2014

Affected Software Version: EOS-4.13.0F through EOS-4.13.1F.

Note: Only publicly accessible systems are vulnerable to this attack.

Bug 77553: ntpd monlist vulnerability

Impact: NTP provides a monitoring service that allows administrators to query an ntpd instance running remotely for a list of up to 600 connected clients and their traffic statistics. A spoofed source address can therefore cause the ntpd instance to send a large amount of UDP traffic to an arbitrary target, which makes publicly accessible NTP servers vulnerable to being used for amplification in DDoS attacks.

Resolution: This is fixed in 4.13.3F.

Workaround: Customers who would prefer not to update to 4.13.3F can modify the control plane ACL to block the NTP port. An example of the general process can be found at Restricting access to the switch. In this case, the line "60 permit udp any any eq bootps bootpc snmp rip ntp" will be replaced by the line "60 permit udp any any eq bootps bootpc snmp rip".

References:
https://www.us-cert.gov/ncas/alerts/TA14-013A