SECURITY ADVISORY

#CVE-2015-7704, -7705, -7871 published on October 23rd, 2015

Summary Description

This security advisory addresses CVE-2015-7704, CVE-2015-7705, and CVE-2015-7871 as they pertain to A10 ACOS software.

On October 21st, the NTP Project[1], released version ntp-4.2.8p4, which among other changes, addresses 13 security vulnerabilities, namely: CVE-2015-7704, CVE-2015-7705, CVE-2015-7871, CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702, CVE-2015-7703, CVE-2015-7848, CVE-2015-7849, CVE-2015-7850, CVE-2015-7851, CVE-2015-7852, CVE-2015-7853, CVE-2015-7854, CVE-2015-7855. Most of the vulnerabilities are ranked at "low" and "medium" level and are described in details in their security advisory[2].

Details

Out of the 13 vulnerabilities only 3 affect ACOS:

- **CVE-2015-7704, CVE-2015-7705** – Denial of Service by Spoofed Kiss-o'-Death – after a successful exploitation, this vulnerability could allow an attacker to disable NTP synchronization of an NTP client. The second vulnerability is a modification of the initial exploit where the attacker primes the server with large number of queries.
- **CVE-2015-7871** – Specially crafted NTP symmetric active crypto-NAK packet, can make a client change its time server to one of the attackers choosing. If successfully exploited this vulnerability would allow an attacker to manipulate the time of a client.

The following CVEs do not affect ACOS:

- **CVE-2015-7691, CVE-2015-7692, CVE-2015-7701, CVE-2015-7702** – ACOS does not allow Autokey
- **CVE-2015-7703, CVE-2015-7849, CVE-2015-7850, CVE-2015-7854, CVE-2015-7855, CVE-2015-7852, CVE-2015-7848** – ACOS does not allow remote configuration

[1] http://www.ntp.org/

[2] http://support.ntp.org/bin/view/Main/SecurityNotice#Recent_Vulnerabilities

- **CVE-2015-7853, CVE-2015-7851** – ACOS does not support the feature being exploited

The A10 QA team has not been able to cause either of those outcomes however patches are being proactively released due to the potential severity of the issue.

Mitigation Recommendations

In regular deployments NTP is only exposed on the management interface and is only supposed to talk to a particular NTP server. This limits the exposure significantly. In addition, it is recommended that access is further limited through Access Control Lists (ACLs). Furthermore, perimeter ACLs should be used to ensure spoofed packets cannot enter the perimeter of the network and impersonate legitimate clients.

Vulnerability Assessment

Affected Platforms: *ADC, CGN, TPS*

Affected Software Versions: *4.x, 3.x, 2.7.2-Px, 2.7.1-GR1, 2.8.2-Px*

Software Updates

Software updates resolving this vulnerability will be published at the following URL when available:

http://www.a10networks.com/support-axseries/downloads/downloads.php

The following table summarizes update versions resolving all of the above CVEs.

Vulnerable Release	Resolved Release
2.7.1-GR1	2.7.1-GR1-P1
2.7.2-Px	2.7.2-P8
2.8.2-Px	2.8.2-P4
3.x	3.3.0[3]
4.x	4.2.0[4]

References

1. NTP Project: http://www.ntp.org/
2. NTP Security Advisory: http://support.ntp.org/bin/view/Main/SecurityNotice#Recent_Vulnerabilities
3. Attacking the Network Time Protocol: https://www.cs.bu.edu/~goldbe/NTPattack.html

[3] Pending upstream patches
[4] Pending upstream patches