RAPID RESPONSE
Security Advisory

SECURITY ADVISORY

#CVE-2014-9293, 9294, 9295, 9296 published on December 29th, 2014

Summary Description

On 19th of December 2014 the Network Time Foundation published a new software release addressing 4 CVEs. The CVEs addressed are:

- CVE-2014-9293 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9293)
- CVE-2014-9294 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9294)
- CVE-2014-9295 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9295)
- CVE-2014-9296 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9296)

This document reflects the response of A10 Networks to the aforementioned vulnerabilities.

The current releases of ACOS include the vulnerable version of the NTP software however there are number of mitigating factors that make the exploitation of those unlikely. In particular there are no cryptographic functions used in the default ACOS NTP configuration. In addition there is no ACOS configuration interface that would allow an end-user to enable any of those features.

The only edge case we believe is exploitable is the buffer overflow in *ctl_putdata()*. However this vulnerability can only be exploited locally or requires a packet with spoofed localhost address to traverse the network which should be mitigated by anti-spoofing filters.

At present the A10 team has not been able to replicate any of the remote buffer overflow issues; however, in the spirit of quality and secure software we are releasing updates. For details refer to the release table below.

Vulnerability Assessment

Affected Platforms: *ADC, CGN, TPS*

Affected Software Versions: *ADC 2.6/2.7/4.0, CGN 2.8/4.0, TPS 2.9/3.0/3.1*

Workarounds

In order to limit the exposure of the software to the buffer overflow vulnerabilities it is recommended that access to the process is limited using access control lists. This will ensure that only systems that are known and trusted to some extent can send traffic to the vulnerable process.

In addition to this ACOS 4.0 by default has the NTP process limited to the management interface only so exploitation through the data-plane should not be possible.

Mitigation Recommendations

A10 Networks recommends upgrading to the latest patches when released. The table below summarizes the software releases resolving that issue.

Vulnerable Release	Resolved Release
3.0.0-TPS-P2-SP15	3.0.0-TPS-P2-SP16
3.1.0-SP1	3.1.0-SP2
3.1.0-P1	3.1.0-P1-SP1
2.9.1-P2-SP26	2.9.1-P2-SP27
2.6.1-GR1-P13	2.6.1-GR1-P14
2.7.0-P6	2.7.0-P7
2.7.1-P6	2.7.1-P6-SP2
2.7.2-P4	2.7.2-P4-SP1
2.6.6-GR1-P6	2.6.6-GR1-P7
2.8.0-P4	2.8.0-P5
2.8.1-P2	2.8.1-P3
2.8.2-P1	2.8.2-P2
4.0.0	4.0.0-P1