ID 20180319 FAQ

Recent Security vulnerabilities addressed by NTP (CVE-2016-1549,CVE-2018-7182,CVE-2018-7170,CVE-2018-7184, CVE-2018-7185, CVE-2018-7183)

Initial Internal Release Date: **03/19/2018**
Initial Release to the public*:* **03/19/2018**
Update Release Date: **03/19/2018**

Summary

Vulnerability Analysis team of CERT (A division of Software Engineering Institute – Carnegie Mellon University) has notified most of the software vendors including Ruckus Networks about the vulnerabilities found in the NTP opensource package version ntp-4.2.8p10. The opensource implementation of NTP Protocol by ntp.org allows for both non-authenticated and authenticated associations, in client/server, symmetric (peer), and several broadcast modes.

The protocol engine in NTP before version 4.2.8p11 allows a remote attacker to cause various vulnerabilities as mentioned in the next sections. Denial of service (disruption) by continually sending a packet with a zero-origin timestamp and source IP address of the "other side" of an interleaved association causing the victim ntpd to reset its association.

What are the issues?

NTP has addressed various vulnerabilities in **ntp-4.2.8p11** which addresses below CVE. These issues were raised by -by various software vendors and researchers was brought to the notice of the CERT, which in turn notified other software vendors. These vulnerabilities are assigned the CVE IDs and details of the same are explained as below:

S. No	CVE-ID	CVE Description
1	CVE-2016-1549	Sybil vulnerability: ephemeral association attack While fixed in ntp-4.2.8p7, there are significant additional protections for this issue in 4.2.8p11
2	CVE-2018-7182	ctl_getitem(): buffer read overrun leads to undefined behavior and information leak
3	CVE-2018-7170	Multiple authenticated ephemeral associations
4	CVE-2018-7184	Interleaved symmetric mode cannot recover from bad state
5	CVE-2018-7185	Unauthenticated packet can reset authenticated interleaved association which can cause a denial of service (disruption) by continually sending a packet with a zero-origin timestamp and source IP address

		of the "other side" of an interleaved association causing the victim ntpd to reset its association.
6	CVE-2018-7183	ntpq:decodearr() can write beyond its buffer limit

How do these vulnerabilities impact Ruckus products?

None of the Ruckus Network products use impacted version ntp-4.2.8p10 and hence are not impacted theoretically. However, products use the older version of ntpd opensource and hence may be potentially vulnerable to these issues. Below table provides the details of the area of impact of each CVE and affected Ruckus products:

SNo.	CVE-ID	Impacted Area	Affected Ruckus Products	Comments
1	CVE-2016-1549	As per CVE's description	All the latest versions of SZ-100, SZ-200, SZ-300, vSZ-E, vSZ-H, Cloudpath, SPoT/vSPoT	All the versions of impacted products are using version older than ntp-4.2.8p10 of ntpd and hence may be impacted.
2	CVE-2018-7182	As per CVE's description	All the latest versions of SZ-100, SZ-200, SZ-300, vSZ-E, vSZ-H, Cloudpath, SPoT/vSPoT	All the versions of impacted products are using version older than ntp-4.2.8p10 of ntpd and hence may be impacted.
3	CVE-2018-7170	As per CVE's description	All the latest versions of SZ-100, SZ-200, SZ-300, vSZ-E, vSZ-H, Cloudpath, SPoT/vSPoT	All the versions of impacted products are using version older than ntp-4.2.8p10 of ntpd and hence may be impacted.
4	CVE-2018-7184	As per CVE's description	All the latest versions of SZ-100, SZ-200, SZ-300, vSZ-E, vSZ-H, Cloudpath, SPoT/vSPoT	All the versions of impacted products are using version older than ntp-4.2.8p10 of ntpd and hence may be impacted.
5	CVE-2018-7185	As per CVE's description	All the latest versions SZ-100, SZ-200, SZ-300, vSZ-E, vSZ-H, Cloudpath, SPoT/vSPoT ICX –7150, 7250, 7450, 7650, 7750	All the versions of impacted products are using version older than ntp-4.2.8p10 of ntpd and hence may be impacted. Ruckus ICX FastIron products running firmware up to version FI 08.0.70 are affected by this vulnerability.
6	CVE-2018-7183	As per CVE's description	All the latest versions of SZ-100, SZ-200, SZ-300, vSZ-E, vSZ-H, Cloudpath, SPoT/vSPoT	All the versions of impacted products are using version older than ntp-4.2.8p10 of ntpd and hence may be impacted.

ID 20180319 FAQ

Are there any workarounds available?
Currently, no workarounds are available for these vulnerabilities and hence customers need to upgrade the impacted products firmware to latest firmware as mentioned in next section. All the CVEs have CVSS base scores which are less than medium level, hence the availability of the fixes or patches with newer version will be provided on the releases on the next available opportunity.

What releases fixes are available?

Platform/Products	Release*	Target Patch Release Date
FastIron(ICX)	FI 08.0.30r FI 08.0.61c FI 08.0.80 FI 08.0.70ba FI 08.0.70c	March 30 2018 April 30 2018 June 2018 April 20 2018 TBD: Release date yet to be planned
SZ-100, SZ-200, SZ-300, vSZ-E, vSZ-H	TBD	TBD. The latest ntp version provided by linux distros is ntp-4.2.6p5. The release number and dates will be updated as soon as the latest ntp-4.2.8p11 patch is available from the linux distribution vendor.
Cloudpath	R5.2R2	TBD. The latest ntp version provided by linux distros is ntp-4.2.6p5. The release number and dates will be updated as soon as the latest ntp-4.2.8p11 patch is available from the linux distribution vendor.
SPoT / vSPoT	SPoT 4.8.0 GA release vSPoT 3.8.0 GA release	The next SPoT and vSPoT releases mentioned are not planned yet. The advisory will be updated with the dates once the releases are planned.

ID 20180319 FAQ

How does Ruckus qualify severity of security issues?

Ruckus Networks typically utilizes the Common Vulnerability Scoring System (CVSS) v3. This rating system is a vendor agnostic, industry open standard designed to convey vulnerability severity and help determine urgency and priority of response. In cases where CVSS v3 scores are not available, CVSS v2 score are provided. Below are the CVSS scores and vector information for respective CVEs:

CVE ID	CVSS 3.0 Base Score	Vector
CVE-2016-1549	5.3 (Medium)	CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N)
CVE-2018-7182	5.3 (Medium)	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVE-2018-7170	3.1(Low)	CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N)
CVE-2018-7184	3.1(Low)	CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L
CVE-2018-7185	3.1(Low)	CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L
CVE-2018-7183	5.0(Medium)	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L

When will this Ruckus Security Advisory be publicly posted?

Ruckus Networks released the initial security advisory to Ruckus field teams on: **03/19/2018**

Ruckus Networks released the initial security advisory to customers on: **03/19/2018**

Public posting: **03/19/2018**

Revision History

ID	Change	Date
20180319	Initial Publication to Ruckus Field Teams	March 19, 2018

Ruckus Support can be contacted as follows:

The full contact list is at: https://support.ruckusNetwork.com/contact-us

DISCLAIMER