Ruckus Wireless Security Advisory ID 123114 FAQ:

Network Time Protocol vulnerability - CVE-2014-9295

Release Date: ***Dec 31, 2014***

This Ruckus Security Advisory constitutes Ruckus Proprietary Information and should not be disseminated, forwarded or disclosed without written permission from Ruckus Wireless.

What is the issue?

A new vulnerability was discovered with Network Time Protocol daemon, ntpd, which is based on multiple stack-based buffer overflows. The weakness exists in ntpd package before 4.2.8 release, which might allow remote attackers to execute arbitrary code via a crafted packet.
Some Ruckus devices use ntpd as NTP server.

How do I check if I am vulnerable?

This issue affects the following software branches and devices. Any products not mentioned in this table are **not** affected.

Affected device	Affected software branch	Notes
SmartCell Gateway	All releases	
Virtual SmartCell Gateway	All releases	

Is there a way to mitigate the vulnerability?

Ruckus recommends that all customers apply the appropriate patch(es) as soon as made available from Ruckus. However, in the event that a patch is either not available from Ruckus or cannot be immediately applied, the following suggestions might help reduce the risk:

- Do not expose administrative interfaces of Ruckus devices to untrusted networks such as the Internet.
- Use a firewall to limit traffic to/from Ruckus device's administrative interface to trusted hosts.
- Use an additional secure tunnel between the various components of the system

How does Ruckus Wireless qualify severity of security issues?

Ruckus Wireless utilizes the Common Vulnerability Scoring System (CVSS) v2. This rating system is a vendor agnostic, industry open standard designed to convey vulnerability severity and help determine urgency and priority of response.

CVSS v2 Base Score: 7.5 (HIGH) (AV:N/AC:M/Au:N/C:P/I:P/A:N)

When will this Ruckus Wireless Security Advisory be publicly posted?

Ruckus Wireless released the initial security advisory to customers and public on **31st December, 2014.**

Where do I download the fixed software patches?

Ruckus customers can obtain the fixed firmware from the support website at https://support.ruckuswireless.com/

Ruckus will provide Hotfix via KSP files for the following releases (any later upgrade images will also have the fix):

Affected device	Affected software branch	Releases qualified for Hotfix via KSP
SmartCell Gateway	1.x, 2.x, 3.x	2.1.1.0.236, 2.1.2.0.146, 2.1.3.0.40, 2.5.1.0.182, 2.6.0.0.402, 3.0.0.0.558
Virtual SmartCell Gateway	2.5.0.1	2.5.0.1.174

Ruckus Support can be contacted as follows:

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