Ruckus Networks - Security Advisory

ID 20180203 FAQ

Java JMX and RMI security vulnerabilities

Initial Internal Release Date: **02/02/2018**
Initial Release to the public***: 02*/13/2018**
Update Release Date: **02/13/2018**

What are the issues?

These vulnerabilities are assigned the CVE IDs and details of the same are explained as below:

CVE ID	CVE Description
CVE-2017-15708	In Apache Synapse, by default no authentication is required for Java Remote Method Invocation (RMI). It allows remote code execution attacks that can be performed by injecting specially crafted serialized objects.
CVE-2016-8735	Remote code execution is possible with Apache Tomcat if JmxRemoteLifecycleListener is used and an attacker can reach JMX ports.

1. CVE-2017-15708: In Apache Synapse, by default no authentication is required for Java Remote Method Invocation (RMI). So Apache Synapse 3.0.1 or all previous releases allow remote code execution attacks that can be performed by injecting specially crafted serialized objects. And the presence of Apache Commons Collections 3.2.1 or previous versions in Synapse distribution makes this exploitable.
2. CVE-2016-8735: Remote code execution is possible with Apache Tomcat before 6.0.48, 7.x before 7.0.73, 8.x before 8.0.39, 8.5.x before 8.5.7, and 9.x before 9.0.0.M12 if JmxRemoteLifecycleListener is used and an attacker can reach JMX ports. The issue exists because this listener wasn't updated for consistency with the CVE-2016-3427 Oracle patch that affected credential types.

What is the impact on Ruckus products?

Ruckus SmartZone products prior to Release 3.6.1 are impacted.

What mitigation steps can I take?

Please take the following actions:

1. It is strongly recommended that all Ruckus SmartZone products must be placed in the DMZ behind a Firewall, if not already done so.
2. The firewall should block the following JMX/RMI ports to render these inaccessible from the internet: 7199, 10103, 10112, 10113, 10116, 10117, 10118, 10119, 10120, 11001.
3. Upgrade the SmartZone software to version 3.6.1 or later to prevent any exploitation of these security vulnerabilities.
4. For SmartZone software prior to 3.6.1, download the corresponding KSP patches from https://support.ruckuswireless.com and apply the same.

What releases or KSP patches will be available with fixes?
SmartZone Release 3.6.1 has the patch integrated into it.
For releases prior to 3.6.1, the following Ruckus KSP patches are available with fixes for the above mentioned vulnerabilities:

Platform	Release*	Target Patch Release Date
SmartZone	3.1.2	Released
	3.2.1	Released
	3.4.2	Released
	3.5.1	Released
	3.6.0	Released

How does Ruckus qualify severity of security issues?
Ruckus Wireless 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-2017-15708	9.8	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2016-8734	6.5	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

When will this Ruckus Security Advisory be publicly posted?
Ruckus Wireless released the initial security advisory to Ruckus field teams on: 02/02/2018
Ruckus Wireless released the initial security advisory to customers on: 02/02/2018
Public posting: 02/09/2018

Revision History

Version	ID	Change	Date
1.0	20180203	Initial Release	February 02, 2018
1.1	20180203	Updated patches target 3.5.1/3.6.0	February 13, 2018

Ruckus Support can be contacted as follows:
The full contact list is at: https://support.ruckuswireless.com/contact-us

DISCLAIMER
THIS RUCKUS NETWORKS SECURITY ADVISORY INCLUDING THE INFORMATION IT CONTAINS AND THE PROGRAMS MADE AVAILABLE THROUGH THE LINKS THAT IT INCLUDES, IS PROVIDED TO YOU ON AN "AS IS" BASIS. RUCKUS NETWORKS (AN ARRIS COMPANY) AND ITS SUPPLIERS DO NOT

WARRANT THAT SUCH INFORMATION OR THE FUNCTIONS CONTAINED IN SUCH PROGRAMS WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE PROGRAMS WILL BE UNINTERRUPTED OR ERROR-FREE. THE INFORMATION AND PROGRAMS ARE PROVIDED TO YOU WITH NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT WILL RUCKUS NETWORKS (AN ARRIS COMPANY), ITS SUPPLIERS, OR ANYONE ELSE WHO HAS BEEN INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THE INFORMATION OR PROGRAMS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION, LOST PROFITS OR LOST DATA, THAT MAY ARISE OUT OF YOUR USE OF OR FAILURE TO USE THE INFORMATION OR PROGRAMS, EVEN IF RUCKUS NETWORKS (AN ARRIS COMPANY) OR SUCH OTHER ENTITIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING SHALL NOT BE DEEMED TO PRECLUDE ANY LIABILITY, WHICH UNDER APPLICABLE PRODUCTS LIABILITY LAW, CANNOT BE PRECLUDED BY CONTRACT.