



OpenSSL 0.9.8, 1.0.0 & 1.0.1 library's vulnerability - CVE-2014-0224

Release Date: **July 07, 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 has been discovered in the popular OpenSSL cryptographic software library. This weakness is detailed in CVE-2014-0224, this issue could be exploited to hijack sessions or obtain sensitive information that were considered protected by the TLS connection, in order to exploit this an attacker need to be able to insert himself between the client & servers, where both client & server need to use an OpenSSL liberally version which is affected by this vulnerability.

Ruckus devices incorporate OpenSSL library to implement various security related features.

Below is list of the affected components:

- Administrative HTTPS Interface (Port 8443)
- AP to SCG Control plane communication (SSH tunnel setup)
- SCG Cluster communication

What are the Pre-requisites for this attack?

The attackers need network to be able to insert a device between the client & server to mount a man in the middle attack, this also required that both client & server side OpenSSL to be running a vulnerable release.

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 Access Points	1.x, 2.x	
Smart Cell Gateway	1.x, 2.x	
ZoneDirector Controllers	9.x and prior	
ZoneFlex Access Points	9.x and prior	

Is there a way to mitigate the vulnerability?

Ruckus recommends that all customers apply the appropriate patch(es) as soon as practical. However, in the event that a patch cannot immediately be 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 (e.g. encrypted tunnel between the AP & the SCG).



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:5.8 (MEDIUM) (AV:N/AC:M/Au:N/C:P/I:P/A:N)

When will this Ruckus Wireless Security Advisory be publicly posted?

Since this vulnerability is a zero day issue already in public domain, Ruckus Wireless is simultaneously releasing the security advisory to customers and public on **Mon 7th July, 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/>

The following patches have the fix (any later patches will also have the fix):

Affected device	Affected software branch	Recommended Patch
SmartCell Access Points	1.x, 2.x	2.1.3.0.26 & following releases
Smart Cell Gateway	1.x, 2.x	2.1.3.0.26 & following releases
ZoneDirector Controllers	9.x and prior	9.7.1.0.32 & following releases
ZoneFlex Access Points	9.x and prior	9.7.1.0.32 & following releases

Ruckus Support can be contacted as follows:

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

THIS RUCKUS WIRELESS 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 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, 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 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.

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

© Copyright 2014 Ruckus Wireless, Inc. All Rights Reserved