Ruckus Wireless Security Advisory ID 031813-2 FAQ:

User authentication bypass vulnerability in ZoneDirector administrative web interface

Customer release date: ***March 25, 2013***
Public release date: ***May 27, 2013***
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 weakness has been discovered in the administrative web interface of the ZoneDirector controller devices. A malicious user with network access to the device's web interface may obtain unauthorized access and perform administrative actions via the web interface.

This issue only applies if ZoneDirector web interface is configured to authenticate admin user via remote authentication methods - RADIUS, LDAP or AD. The user does not have to be authenticated to the web interface for this attack to be successful. This issue does not affect any other Ruckus devices besides ZoneDirector controllers.

What are the Pre-requisites for this attack?

This issue is applicable only in certain configuration

- This issue is applicable ONLY if ZoneDirector administrative web interface is configured to authenticate admin user via remote authentication methods: RADIUS, LDAP or AD.

- ZoneDirector controller is NOT vulnerable if local authentication or TACACS is being used for authenticating admin user to the web interface.

- No other Ruckus devices are vulnerable to this issue besides ZoneDirector controllers.

How do I check if I am vulnerable?

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

Ruckus Device	Affected software branch
ZoneDirector Controllers	9.3.x, 9.4.x, 9.5.x

Is there a way to mitigate the vulnerability?

Ruckus Wireless 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 steps will help to mitigate the risk:

- Do not expose management interfaces of Ruckus devices (including administrative web interface) to untrusted networks such as the Internet.
- Use a firewall to limit traffic to/from ZoneDirector's administrative web interface to trusted hosts.
- Switch to using local authentication or TACACS for ZoneDirector administrative web interface.

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 METRIC SCORE: 8.8 (AV:N/AC:M/Au:N/C:C/I:C/A:N)

When will this Ruckus Wireless Security Advisory be publicly posted?

In order to protect our customers and partners, we allow time for customers to upgrade systems or implement workarounds to minimize the vulnerability risk. The security advisory will be posted on publicly on **May 27, 2013.** This Ruckus Security Advisory constitutes Ruckus Proprietary Information and should not be disseminated, forwarded or disclosed without written permission from Ruckus Wireless.

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 software branch	Software Patch
9.3.x	9.3.4.0.17
9.4.x	9.4.3.0.16
9.5.x	9.5.1.0.50

Ruckus Support can be contacted as follows:

1-855-RUCKUS1 (1-855-782-5871) (United States)
e-mail: support@ruckuswireless.com

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