Ruckus Wireless Security Advisory ID 111113-2 FAQ:

Authenticated persistent cross site scripting vulnerability in guest pass provisioning web interface on ZoneDirector controllers

Customer release date: ***Sep 9, 2013***
Public release date: ***Nov 11, 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 persistent cross site scripting vulnerability has been discovered in guest pass provisioning web interface on ZoneDirector controllers (ZD). For launching this attack, the attacker needs access to an authenticated user session with privileges for guest pass generation.

What are the Pre-requisites for this attack?

The pre-requisite of this attack is that attacker has access to an authenticated user session with privileges for guest pass generation on the ZD. This issue does not affect any other Ruckus devices besides ZoneDirector controllers.

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.

Ruckus Device	Affected software branch
ZoneDirector Controllers	9.3.x, 9.4.x, 9.5.x, 9.6.x
ZoneFlex Access Points	NOT AFFECTED
SmartCell Access Points	NOT AFFECTED
Smart Cell Gateway	NOT AFFECTED

Is there a way to mitigate the vulnerability?

Ruckus recommends that all customers apply the appropriate patch(es) as soon as practical for mitigating this attack. However, in the event that a patch cannot immediately be applied, the following suggestions might help reduce the risk:

- Only launch web sessions to ZD's guest pass provisioning interface from trusted hosts with no connectivity to untrusted networks such as the Internet while the session is active.

- Do not expose ZD's guest pass provisioning interface to untrusted networks such as the Internet.

- Use a firewall to limit traffic to/from ZoneDirector's guest pass provisioning web interface to trusted hosts.

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: 4.9 (AV:N/AC:M/Au:S/C:P/I:P/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 **Nov 11, 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	Recommended For
9.3.x	9.3.4.0.21	ZoneDirector 1000
9.4.x	9.4.3.0.22	ZoneDirector 1100/3000/5000
9.5.x	9.5.2.0.15	Standalone Access Points ZoneDirector 1100/3000/5000
9.6.x	9.6.1.0.15	Standalone Access Points ZoneDirector 1100/3000/5000

Ruckus Support can be contacted as follows:

1-855-RUCKUS1 (1-855-782-5871) (United States)

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