# Authenticated Root Command Injection Vulnerabilities in Web-GUI of Ruckus Zone Director Controller and Unleashed APs (CVE-2017-6223, CVE-2017-6224)

Initial Internal Release Date: **09/29/2017**
Initial Release to the public*:* **09/29/2017**
Update Release Date: **09/29/2017**



## Summary

Ruckus Wireless's Zone Director Controller and Unleashed APs firmware contain vulnerabilities that could allow authenticated valid users to execute privileged commands on the respective systems. Moreover, due lack of CSRF protection, in special cases, a remote unauthenticated attacker could also achieve arbitrary command execution as root by convincing an authenticated user to open malicious web content. These vulnerabilities were first reported by Tripwire (organization providing cyber security solutions www.tripwire.com) and Ruckus Wireless acknowledges them unconditionally. Ruckus Wireless has released fixes for these vulnerabilities via software updates, since workaround(s) are not available to mitigate the same.

## What are the issues?

**Authenticated Root Command Injection**: is a type of vulnerability in the Web-GUI that allows an authenticated and valid user to carry out an attack by executing arbitrary privileged commands on the underlying operating system of the affected system as well as on underlying operating system of the devices associated and managed by the affected system.

This vulnerability is introduced due to a failure in properly sanitizing the user input and that is subsequently used to perform an action using the underlying command-line or shell interface of the device. For instance, the attacker after login to Web-GUI could exploit this vulnerability and append arbitrary code or commands to some of values passed to the system which may lead to undesired results. Tripwire reported that Ruckus Wireless Zone Director Web-GUI's 'ping' window is affected where the user can input any Linux command along with shell escape characters, and the command is executed after the ping command execution. Similar weakness is reported by the Tripwire for the Unleashed APs 'Certificate Generation Request' window where the arbitrary commands are appended in Common Name field leading to execution of the command. Due to lack of CSRF protection, in special cases, these vulnerabilities could also be exploited by an unauthenticated attacker by tricking a valid user to execute RCE.

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

| SNo. | CVE-ID | Title |
|---|---|---|
| 1 | CVE-2017-6223 | Zone Director Firmware is prone to authenticated root command injection in the ping functionality. |
| 2 | CVE-2017-6224 | Zone Director and Unleashed AP Firmware are prone to authenticated root command injection via the certificate request generation process window. |

# ID 092917 FAQ

## What is the impact of this for Ruckus products?

a) **Impact of CVE-2017-6223:** Zone Director firmwares that are impacted due to CVE-2017-6223 are ZD9.9.x, ZD9.10.x, ZD9.12.x, ZD9.13.0.x but less than 9.13.0.0.232. In general, all the GA firmware which were released before August 2016 are impacted due to this vulnerability.

b) **Impact of CVE-2017-6224:** Zone Director firmwares that are impacted due to CVE-2017-6224 are ZD9.x, ZD10.0.0.x, ZD10.0.1.x (less than 10.0.1.0.17 MR1 release). Unleashed AP firmwares that are impacted due to CVE-2017-6224 are 200.0.x, 200.1.x, 200.2.x, 200.3.x, 200.4.x.

## Workaround available?

Currently, no workarounds are available for these two vulnerabilities and hence customers need to upgrade the Zone Director and Unleashed AP firmware to latest firmware as mentioned in next section.

## What releases fixes are available?

| CVE ID | Status | Release / Comments |
|---|---|---|
| CVE-2017-6223 | Fix for ZD1200 and ZD3000 is available. | For Release 9.13.3.x, fix is available in build **9.13.3.0.121 (MR3 Refresh3)** and above. For release 10.0.0.x and 10.0.1.x fix is available in build **10.0.1.0.17(MR1)** and above. All the upcoming GA releases of Zone Director shall contain the fixes. |
| CVE-2017-6224 | - Fix for ZD 1200 and ZD300 is available.<br><br>- Fix for Unleashed APs is planned in next 200.5.x GA release shortly. | - For ZD release 9.13.3.x, fix is available in build 9.13.3.0.121 (MR3 Refresh3) and above. For release 10.0.0.x and 10.0.1.x fix is available in build **10.0.1.0.17(MR1)** and above. All the upcoming GA releases of Zone Director shall contain the fixes.<br><br>- For Unleashed APs fix is available in build **200.5.10.0.225** and above. This build is planned to be released as part of 200.5.x GA release shortly. |

## How does Ruckus Wireless 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-2017-6223 | 7.6 (High) | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H |
| CVE-2017-6224 | 7.6 (High) | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H |

# ID 092917 FAQ

## When will this Ruckus Wireless Security Advisory be publicly posted?

Ruckus Wireless released the initial security advisory to Ruckus field teams on: **09/29/2017**

Ruckus Wireless released the initial security advisory to customers on: **09/29/2017**

Public posting: **09/29/2017**

### Revision History

| ID | Change | Date |
|---|---|---|
| 092917 | Initial Publication | September 29, 2017 |

## Ruckus Support can be contacted as follows:

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

## DISCLAIMER