ID 20180202 FAQ

Authenticated Root Command Injection Vulnerabilities in CLI of ZD/Unleashed APs and Web-GUI of Solo/SZ Managed APs (CVE-2017-6229, CVE2017-6230)

Initial Internal Release Date: **02/02/2018**
Initial Release to the public**: 02/09/2018**
Update Release Date: **02/02/2018**

Summary

Ruckus Network's Zone Director, Unleashed, Solo and SZ APs contain vulnerabilities that could allow authenticated valid users to execute privileged commands on the respective systems. 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 reported by TigerPuma *(Independent security researcher tigerpuma@fosec.vn)* and Ruckus Networks acknowledges them unconditionally. Ruckus Networks is planning to release fixes for these vulnerabilities via software updates.

What are the issues?

Authenticated Root Command Injection is a type of vulnerability in the CLI and 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 interface of the device. For instance, the attacker after login to CLI (using "ping" command) and 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. TigerPuma reported that Ruckus Networks Zone Director and Unleashed APs CLI 'ping' command 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. Also in the solo APs and SZ managed APs, Web-GUI's the tftp upgrade page allows to input arbitrary commands due to lack of input validation. However, SZ managed APs are only impacted if they have lost communication with the SZ.

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

SNo.	CVE-ID	CVE Description
1	CVE-2017-6229	Authenticated command injection in CLI interface of ZD/Unleashed software.
2	CVE-2017-6230	Authenticated command injection in WebUI interface of Solo and managed AP via tftp upgrade option.

ID 20180202 FAQ

How do these vulnerabilities impact Ruckus products?
Below table provides the details of the area of impact of each CVE and affected Ruckus products:

SNo.	CVE-ID	Affected Ruckus Products	Comments
1	CVE-2017-6229	Ruckus Unleashed APs Ruckus ZD	All models of unleashed AP are impacted which have release before: 200.6.10.1.x All models of ZD are impacted which have following release version(s) or *before:* 10.1.0.0.x, 9.10.2.0.x, 9.12.3.0.x, 9.13.3.0.x, 10.0.1.0.x
2	CVE-2017-6230	All Solo APs All SZ managed APs are impacted only if the APs have lost communication with SZ.	All solo APs are impacted which have following release version(s) or before: R110.x All SZ APs are impacted which have following release version(s) or before: R5.x Note: Workaround is available for avert this vulnerability. Refer workaround section below.

Are there any workarounds available?
Currently, no workarounds are available for CVE-2017-6229 vulnerability and hence customers need to upgrade the Zone Director, Unleashed APs to the release(s) which contains the fixes.

For SZ Managed APs the CVE-2017-6230 shall impact only if the AP loses communication with the SZ.
For both SZ and Solo APs workaround is available for CVE-2017-6230 which is to disable the UI interface via CLI with following steps:

i) Login to AP via SSH with AP IP and input username and password.
ii) After successful authentication, CLI interface of the Ruckus AP will be displayed. Check the status of https and http service with following CLI commands “get https” and “get http”
iii) If any of the two services are running, then bring down both the services by executing following CLI commands: “set https disable” and “set http disable”.
iv) Verify the status of the service by executing the commands mentioned in step iii above and ensure that both are disabled. If both the services are disabled, type exit to close the SSH session

Note: After disabling the https and http services, AP GUI will be unavailable, and AP can then be controlled or configured via CLI interface ONLY.

ID 20180202 FAQ

What releases fixes are available?

Platform/Products	Release*	Target Patch Release Date
SZ AP	SZ3.4.2 (Patch3) SZ3.6.1 GA SZ5.0 GA	April 2018. April 2018. SZ5.0 GA release is scheduled for second quarter of 2018
ZoneDirector	10.1.0.0, 9.10.2.0, 9.12.3.0, 9.13.3.0, 10.0.1.0 or *later*	These releases are already available in the support portal of Ruckus. Contact support for the same.
UN AP	200.6.10.1 or *later*	April' 2018
Solo AP	R110.0 GA	R110.0 GA release is scheduled to be available during second quarter of 2018.

ID 20180202 FAQ

How does Ruckus qualify severity of security issues?

Ruckus Networks 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-2017-6229	7.6 (High)	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H
CVE-2017-6230	7.6 (High)	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H

When will this Ruckus Security Advisory be publicly posted?

Ruckus Networks released the initial security advisory to Ruckus field teams on: **02/02/2018**

Ruckus Networks released the initial security advisory to customers on: **02/02/2018**

Public posting: **02/09/2018**

Revision History

ID	Change	Date
20180202	Initial Publication to Ruckus Field Teams and customers	February 2nd , 2018

Ruckus Support can be contacted as follows:

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

DISCLAIMER