# Ruckus Networks - Security Advisory
# ID 20190412 FAQ

## Dragonblood Vulnerabilities – VU#871675

CVE-2019-9494
CVE-2019-9495
CVE-2019-9496
CVE-2019-9497
CVE-2019-9498
CVE-2019-9499

Initial Internal Release Date: **04/12/2019**
Initial Release to the public*:* **04/12/2019**
Update Release Date: **04/12/2019**



### Summary

Security researchers have reported new vulnerabilities in the WPA3-Personal protocol. Simultaneous Authentication of Equals (SAE) handshake, a.k.a Dragonfly vulnerabilities could be exploited to perform DOS attack or to gain access to the network and attack the EAP-pwd server or peer. For more detail about these vulnerabilities, please refer here:

https://wpa3.mathyvanhoef.com

### What are the issues?

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

| CVE ID | CVE Description |
|---|---|
| VU#871675 | Denial of Service attack against Dragonfly handshake and downgrade attack against WPA3 transition mode leading to dictionary attack. |
| CVE-2019-9494 | Cache-based side-channel attack against Dragonfly handshake. |
| CVE-2019-9495 | Cache-based side-channel attack against EAP-pwd. |
| CVE-2019-9496 | SAE confirm missing state validation could cause hostapd process termination, which can be exploited to perform DOS attack. |
| CVE-2019-9497 | EAP-pwd server missing commit validation for reflection attack can be exploited to complete authentication without password but cannot derive the session key to complete the 4-way handshake. |
| CVE-2019-9498 | EAP-pwd server missing commit validation for scalar can be exploited to gain access to the network and derive session keys and perform more sophisticated attacks on EAP server. |
| CVE-2019-9499 | EAP-pwd peer missing commit validation for scalar can be exploited to gain access to the network and derive session keys and perform more sophisticated attacks on EAP peer. |

**What is the impact on Ruckus products?**
No Ruckus products are impacted as WPA3 authentication shall be available in SmartZone, ZD and Unleashed from Releases marked below with appropriate security patches integrated.

| Platform | Release* | Target Patch Release Date |
|---|---|---|
| SmartZone | 5.1 or Before | No Impact |
| | 5.2 | Oct 2019 |
| ZoneDirector | 10.2 or Before | No Impact |
| | 10.3 | Jul 2019 |
| Unleashed | 200.7 or Before | No Impact |
| | 200.8 | TBD |
| Cloud | 18.04 or Before | No Impact |

**What is the impact on Ruckus ICX, Brocade FastIron and TurboIron switches that are part of Ruckus now?**
No Ruckus ICX, Brocade FastIron and TurboIron switches are impacted.

**What action do I take?**
No immediate action is required.

Ruckus is actively investigating available hostapd security patches and other mitigations and would deploy these in software releases marked above. Ruckus is doing the due diligence to test the impact of these patches on our quality, performance and resiliency.

## Revision History

| Version | ID | Change | Date |
|---|---|---|---|
| 1.0 | 20190412 | Initial Release | April 12, 2019 |

## Ruckus Support can be contacted as follows:

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

## DISCLAIMER

THIS RUCKUS NETWORKS 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 NETWORKS (AN ARRIS COMPANY) 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 NETWORKS ( AN ARRIS COMPANY), 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 NETWORKS (AN ARRIS COMPANY) 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.