# ID 20180816 FAQ

# Dictionary attacks on WiFi Protected Access (WPA & WPA2) Protocols

Initial Internal Release Date: **08/16/2018**
Initial Release to the public**: 08/16/2018**
Update Release Date: **08/16/2018**



## Summary

Jens "Atom" Steube from the Hashcat project, recently published an article describing a method that can aid cracking the Wireless pre-shared key(PSK) offline, by capturing a EAPOL frame with Robust Security Network Information Element (RSN IE) PMKID. The article is available here: https://hashcat.net/forum/thread-7717.html

## What is the issue?

The article identifies a new vector for gathering information, which in turn can be utilized to perform a dictionary attack offline to crack the wireless PSK.
It should be noted that WPA/WPA2 passphrases have been inherently subject to computational/algorithmic methods of hacking, lately. The amount of computational effort required to crack a WPA/WPA2 hashed Wi-Fi Network passphrase is directly proportional to the length, uniqueness, and complexity of the passphrase.
Ruckus is in agreement with WiFi Alliance's statement that has been attached to the Appendix section of this advisory, which emphasizes the same.

## What is the impact on Ruckus products?

No Ruckus products are vulnerable. This is because Ruckus does not add the optional RSN IE to the EAPOL packets exchanged during the 4-way authentication handshake.
Nevertheless, the best method of protection is to ensure strong passphrases are used. Ruckus recommends the following best practices:

- Use passwords with 16 characters or more, using combination of upper/lower case, numeric, and special characters and use a password generator wherever possible.
- Use Ruckus DPSK, which assigns each user a unique PSK, if stronger security than shared PSK is desired.
- Enable 802.11w to further enhance the security.
- Use WPA3 that provides a unique PMK per user, when available.

# ID 20180816 FAQ

**Revision History**

| Version | ID | Change | Date |
|---|---|---|---|
| 1.0 | 20180816 | Initial Release | August 16, 2018 |

**Ruckus Support can be contacted as follows:**

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

**APPENDIX**

**From:** wfa-securitymarketing@groups.wi-fi.org <wfa-securitymarketing@groups.wi-fi.org> **On Behalf Of** Kevin Robinson
**Sent:** Tuesday, August 07, 2018 4:15 PM
**To:** wfa-vrt@groups.wi-fi.org
**Cc:** wfa-securitymarketing@groups.wi-fi.org
**Subject:** [wfa-securitymarketing] WPA2 PMKID Attack Response

Dear Vulnerability Review Team Participants: (Security MTG copied)

Wi-Fi Alliance has been monitoring the recent news coverage on the PMKID-based WPA2 attack. Based on staff outreach to members and recent discussions on the VRT reflector, the points below summarize our understanding of the general situation:

- A dictionary attack against a Wi‑Fi network PMKID does not significantly reduce the effort from what is required to successfully execute a dictionary attack on the four-way handshake.
- There are a number of means by which an attacker could initiate a dictionary attack, and this approach simply provides a different way for an attacker to collect the inputs necessary to execute that attack.
- Quality of the network password remains a key element in preventing password guessing attempts on a WPA2-Personal network, and users should always choose strong passwords.
- The key establishment protocol in WPA3-Personal provides protections against offline dictionary attacks, and its use of a PMKID is not susceptible to this attack because it is not based on the PMK.

At this time, there is no plan to conduct proactive media outreach. However, Wi-Fi Alliance has prepared the drawer statement below in response to any potential media inquiries. Members are encouraged to align with this statement if they receive media inquiries.

Staff feels we have sufficient information to respond to this event without the need to schedule a Vulnerability Review Team (VRT) call. If the situation changes or members determine more analysis is required, the Security MTG leadership may schedule a Vulnerability Review Team call.

# ID 20180816 FAQ

**Statement:**

*This is an alternate approach for collecting the inputs for a standard dictionary attack and does not significantly change the effort required to actually run the dictionary attack. However, it does serve as a reminder of the importance of choosing strong network passwords that are not susceptible to guessing attempts.*

*With the introduction of WPA3, Wi‑Fi Alliance is delivering the next generation of Wi‑Fi security with enhanced protections for personal and enterprise networks. WPA3-Personal provides more robust password-based authentication making it resistant to offline dictionary attacks, even when users choose passwords that fall short of typical complexity recommendations.*

**Attack reference:**

Hashcat.net - https://hashcat.net/forum/thread-7717.html

**Sample Coverage:**

New Wi-Fi crack attack allows outsiders to snag user creds
**ITNews**
Researchers have accidentally discovered a new attack on the Wi-Fi protected access protocols used in wireless access points that makes it easier for outsiders to capture access credentials. Hashcat developer Jens "Atom" Steube explained to iTnews that the biggest difference between the new method and prior WPA/WPA2 cracks is that an attacker no longer needs another user to be on the target network to capture credentials - "simply starting the authentication process will do."
**Additional coverage:** Security Boulevard, Bleeping Computer, TechRepublic, The Register, and more

Regards,
Kevin

**Kevin Robinson**
Vice President, Marketing
Wi-Fi Alliance

# ID 20180816 FAQ

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.