



**TLP:WHITE**  
**Szabadon terjeszthető!**

## **Riasztás** **WPA3 protokoll sérülékenységeinek kihasználása**

(2019.04.12.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet riasztást ad ki a **WPA3 protokoll újonnan felfedezett sérülékenysége miatt**.

Az úgynevezett **Dragonblood** sérülékenységek között egy DoS támadást lehetővé tevő sérülékenység, két Downgrade Attack sérülékenység, valamint két side-channel információ szivárgás sérülékenység található.

Míg a DoS támadást lehetővé tevő sérülékenység a WPA3 kompatibilis Access Point-ok leállításához vezet, addig a többi négy sérülékenységet felhasználva a támadók visszafejthetik az áldozat WiFi jelszavát és hozzáférhetnek annak hálózatához.

A Downgrade Attack sérülékenységek esetén a WPA3 kompatibilis hálózatot arra kényszerítik, hogy egy régebbi, kevésbé biztonságos jelszó cserélő rendszert használjon, ezáltal annak hibáit kihasználva tudják kinyerni a hálózat jelszavát.

A két side-channel információ szivárgás sérülékenység esetén a WPA3 kompatibilis eszközt ráveszik arra, hogy gyengébb algoritmust használva információt szivárogtasson a hálózati jelszóról. A támadások ismétlésével a teljes jelszó visszafejthető.

A WPA3 sérülékenységét felfedező biztonsági szakértők felhívták a figyelmet az EAP-pwd elleni támadás veszélyeire is, amelyről részletes információt nem közölnek annak kijavításáig.

### **WPA3 sérülékenységek javítása**

A WiFi Alliance bejelentette, hogy elkészítették a WPA3 protokoll biztonsági frissítését, melyet a gyártók már beépíthetnek szoftver frissítéseikbe. A frissítések megjelenéséig a rendszerek sérülékenysége az alábbi szkriptek segítségével tesztelhető.

- [Dragonslayer](#)
- [Dragonrain](#)
- [Dragontime](#)
- [Dragonforce](#)

**További információ az alábbi hivatkozáson érhető el:**

- <https://www.wi-fi.org/security-update-april-2019>

**A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet a biztonsági frissítések haladéktalan telepítését javasolja.**

A Nemzeti Kibervédelmi Intézet hazai szintén is szerepet vállal a felhasználók informatikai biztonsági tudatosításában. Ennek érdekében minden héten egy tájékoztató, figyelem felhívó Nemzetközi IT-biztonsági sajtószemlével<sup>1</sup> jelentkezik, valamint tudatosító anyagokat tesz közzé honlapján ([nki.gov.hu](http://nki.gov.hu)).

**Nemzetbiztonsági Szakszolgálat**

**Nemzeti Kibervédelmi Intézet**

Telefon: +36-1-336-4833

Fax: +36-1-336-4886

Incidensbejelentés: [cert@nki.gov.hu](mailto:cert@nki.gov.hu)



---

<sup>1</sup> <https://nki.gov.hu/it-biztonsag/kiadvanyok/sajtoszemle/>