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 tévő 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 leállásához 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
- Dragondrain
- 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 színtéren is szerepet vállal a felhasználók informatikai biztonsági tudatosításában. Ennek érdekében minden héten egy tájékoztató, figyelem felhívó Nemzetközi IT-biztonsági sajtószemlével[1] jelentkezik, valamint tudatosító anyagokat[2] tesz közzé honlapján (itbiztonsag.govcert.hu).

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Fax: +36-1-336-4886
Incidensbejelentés: cert@nki.gov.hu

[1] https://itbiztonsag.govcert.hu/dokumentumok/sajtoszemle
[2] https://itbiztonsag.govcert.hu/dokumentumok/kiadvanyok