Draytek

DrayTek security melding

Recent werden we ons bewust van nieuwe aanvallen op web-enabled apparaten, waaronder DrayTek-routers. De recente aanvallen hebben geprobeerd de DNS-instellingen van routers te wijzigen.

Onderzoek heeft uitgewezen dat dit in een aantal gevallen ook daadwerkelijk succesvol is gelukt.

Om deze reden willen wij u met klem adviseren om alle DrayTeks die u in uw netwerk heeft te controleren en te updaten.

Risico

Het wijzigen van uw DNS-serveradres lijkt misschien een vreemde en zeer onbeduidende omgeving voor een hacker om te veranderen.

Als iemand u doorverwijst naar een malafide DNS-server, kunnen zij uw browser, zonder dat u daar erg in heeft, naar een nepsite leiden, terwijl u denkt dat u naar uw favoriete website gaat.

De oplettende gebruiker ziet dat:

- de URL niet klopt (vaak is er slechts een heel klein verschil met de URL die hij/zij wil bezoeken),
- de URL begint met http:// in plaats van https:// (waarbij de S staat voor secure),
- deze websites niet voorzien zijn van een ‘slotje’.

Mocht u op een dergelijke nepsite inloggen dan hebben de criminelen uw gebruikersnaam en wachtwoord, met alle gevolgen vandien.

Welke acties moet u ondernemen?

- Wij adviseren om alle DrayTek modem/routers te voorzien van de laatst beschikbare firmware. Daarnaast blijft het advies om remote management enkel met een access list te gebruiken, als u daadwerkelijk remote beheer dient uit te voeren.
- Controleer of de DNS (check alle LANs) of deze aangepast is naar: 38.134.121.95 en als secundaire dns 8.8.8.8. Deze informatie is standaard niet gevuld, dus als dat wel het geval is. dient u de dns instellingen te verwijderen of aan te passen naar valide dns servers.
  Via https://www.draytek.co.uk/support/security-advisories/kb-advisory-csrf-and-dns-dhcp-web-attacks vindt u een stappenplan hoe u dit kunt controleren/aanpassen.
- We raden u aan om wachtwoorden te wijzigen van websites die u onlangs hebt bezocht, met name financiële wachtwoorden, en uw router- en WiFi-wachtwoord(en).

Download Firmware

Hieronder een overzicht met de firmware-versies die over een patch beschikken.

- Vigor2120, versie 3.8.8.2
- Vigor2132, versie 3.8.8.2
- Vigor2133, versie 3.8.8.2
- Vigor2760, versie 3.8.8.2
- Vigor2762, versie 3.8.8.2
- Vigor2860, versie 3.8.8
- Vigor2862, versie 3.8.8.2
- Vigor2862B, versie 3.8.8.2
- Vigor2925, versie 3.8.8.2
- Vigor2926, versie 3.8.8.2
- Vigor2952, versie 3.8.8.2

Via http://draytek.nl/downloads/firmware/ kunt u de laatste versies van de firmware downloaden.

Voor modellen waar nog geen firmware update beschikbaar is, adviseren wij remote management uit te schakelen of deze ten minste te gebruiken in combinatie met een access list. Firmwares voor deze modellen zullen spoedig beschikbaar worden gesteld op www.draytek.nl.

Voor de modellen die al geruime tijd ‘end of life’ zijn is het nog niet duidelijk of DrayTek daar op korte termijn een nieuwe firmware versie voor beschikbaar gaat stellen. Wij willen u, als het om een dergelijk model gaat, adviseren om een nieuwe model te plaatsen of zelf maatregelen te treffen dat de modems niet misbruikt kunnen worden.

Unieke FAQ ID: #1449
Auteur:
Laatst bijgewerkt:2018-05-25 11:44