10 jul 2020 -12:10

Het CCB waarschuwt voor potentiële Ransomware-aanval

Het Centrum voor Cybersecurity België (CCB) heeft uit betrouwbare bron informatie ontvangen die wijst op een niet-geïdentificeerde kwetsbaarheid in DrayTek-routers, waardoor ransomware-aanvallers toegang zouden krijgen tot duizenden bedrijfsnetwerken wereldwijd.

Een onderzoek van het Centrum voor Cybersecurity België (CCB) wijst uit dat DrayTek Vigor2960-routers zeker zijn getroffen door de niet-geïdentificeerde kwetsbaarheid. Het is niet uitgesloten dat de kwetsbaarheid ook nog andere DrayTek toestellen treft.

De kwetsbaarheid stelt de aanvaller in staat om de authenticatieprocedures te omzeilen en op afstand code te injecteren of/uit te voeren op het besturingssysteem van de DrayTek Vigor2960-routers.

DrayTek ontwikkelde inmiddels patches voor sommige recentelijk bekendgemaakte beveiligingskwetsbaarheden, maar het is niet duidelijk of de eerder genoemde misbruikte kwetsbaarheid is gepatcht. Het CCB beveelt gebruikers evenwel sterk aan de laatste beveiligingsupdates uit te voeren op DrayTek- routers.

Controleer op backdoors

Het CCB heeft penetratietesten uitgevoerd, waaruit blijkt dat eerder geïnstalleerde backdoors op Vigor2960-routers, waarbij gebruik werd gemaakt van versie 1.4 van de firmware, niet werden verwijderd na het patchen naar versie 1.5.1.1. Dit suggereert dat een gecompromitteerde router ook na het upgraden naar versie 1.5.1.1 gecompromitteerd zal blijven.

> "“We roepen bedrijven op om getroffen toestellen te updaten en te controleren op backdoors. De uitvoering van de beveiligingsupdate van DrayTek is in dit geval geen garantie dat je niet kwetsbaar meer bent voor de potentiële ransomware-aanval. Als hackers vooraf aan de update backdoors konden installeren, dan ben je ook na de patch nog kwetsbaar”"
>
> Pedro Deryckere
> Centrum voor Cybersecurity België

Het CCB heeft de belanghebbenden een specifieke beveiligingswaarschuwing gestuurd met de beschrijving, mogelijke gevolgen en mogelijke oplossingen van de kwetsbaarheid en de dreiging.

Te ondernemen acties:

- Maak altijd een back-up van je configuratie vooraleer je een upgrade doet.
- Upgrade je apparaten onmiddellijk en controleer ze op eventuele nieuwe patches voor de DrayTek-apparaten.
- Controleer na de upgrade of de web interface nu de nieuwe firmware-versie toont.
- Controleer of er geen bijkomende profielen voor toegang op afstand (VPN-login, telewerker of LAN to LAN) of admin users (voor router admin) zijn toegevoegd.
- Controleer of er ACL's (Access Control Lists) gewijzigd zijn.
- Schakel de toegang op afstand op je router uit als je hem niet nodig hebt.
- Schakel de toegang op afstand (admin) en SSL VPN uit. De ACL is niet van toepassing op SSL VPN-verbindingen (Poort 443), dus je moet ook SSL VPN tijdelijk uitschakelen tot je de firmware hebt geüpdatet.
- Schakel syslog-logging in om te controleren op abnormale gebeurtenissen.

Het CCB heeft DrayTek gecontacteerd en geïnformeerd maar kreeg geen antwoord.

Ransomware is aan een opmars bezig

Ransomware is een virus dat wordt geïnstalleerd op een toestel zonder dat de eigenaar daarvoor toestemming gaf en vraagt losgeld in ruil voor het deblokkeren van apparaten en bestanden.

Iedereen kan het slachtoffer worden van ransomware: van particulieren tot zelfstandige beroepsbeoefenaars, ziekenhuizen en zelfs grote bedrijven en de overheid.

Je kan jezelf beschermen tegen ransomware

Voor alle internetgebruikers:

- Het is belangrijk om je apparaten te beveiligen met antivirussoftware, maar ook specifieke bescherming tegen ransomware is een must geworden.
- Ook is het nog altijd heel belangrijk om valse berichten tijdig te identificeren en regelmatig updates te maken van al je systemen.
- Maak tot slot ook regelmatig back-ups voor het geval je met een aanval te maken krijgt.

Voor ondernemingen en organisaties:

- De aanbevelingen voor alle internetgebruikers zijn uiteraard ook belangrijk voor ondernemingen en

organisaties, maar we raden hun aan om een stap verder te gaan.

- Voor kmo's en zelfstandigen kan Endpoint-beschermingssoftware voldoende zijn. Maar voor grote bedrijven is een gespecialiseerde professionele anti-ransomwareoplossing aan te bevelen.
- Zorg voor een bedrijfscontinuïteits- en herstelplan met een getest back-upsysteem.
- Zorg dat je organisatie voorbereid is op een cyberaanval. Bekijk onze webinar.
- Laat je IT-beveiligingsarchitectuur & -beleid beoordelen door een specialist (inclusief beleid inzake patching, gebruikerstraining, netwerksegmentatie etc.).
- Maak werk van een cybersecuritystrategie. Lees hier hoe je dat kan doen.

Privégebruikers vinden alle nodige tips om zich te beschermen tegen ransomware op www.safeonweb.be.

Organisaties en ondernemingen kunnen terecht op www.CERT.be. In september 2019 hebben we de *Whitepaper* 'Ransomware: bescherming en preventie' gepubliceerd. Deze Whitepaper werd geüpdatet in 2020.

Centrum voor Cyber Security België
Wetstraat 16
1000 Brussel
België
http://www.ccb.belgium.be

Andries Bomans
Communicatieverantwoordelijke
+32 471 66 00 06
andries.bomans@ccb.belgium.be

Katrien - momenteel in verlof Eggers - momenteel in verlof
Communicatieverantwoordelijke
+32 485 76 53 36
katrien.eggers@cert.be