Reacties op het rapport digitale veiligheid IoT-apparatuur

Toelichting

Om inzicht te krijgen in de huidige staat van de beveiliging van IoT-consumentenapparaten heeft Agentschap Telecom de digitale beveiliging van deze apparatuur op de Nederlandse markt onderzocht. 22 Veel gebruikte IoT-consumentenapparaten zijn onderzocht binnen een aantal productgroepen. Het betrof een willekeurige steekproef bij de grootste verkoopketens in Nederland. Dit betekent dat er ook andere – niet geteste – apparatuur is waar problemen kunnen spelen.

Reacties

Hieronder worden de ontvangen reacties van de onderzochte merken weergegeven. De contactpersonen zijn bij Agentschap Telecom bekend.

ROUTERS

TP-Link Archer C3150
TP-Link streeft naar producten die volledige veiligheid garanderen. Door middel van firmware updates zijn wij dagelijks bezig met het verbeteren van deze veiligheid voor al onze producten. Naar aanleiding van de bevindingen van het agentschap voor de telecom hebben wij een aantal verbeteringen doorgevoerd. Wij verwelkomen dergelijke tips en moedigen iedereen aan deze ook te melden. TP-Link is van mening dat het installeren van een firmware update de keuze van de consument moet zijn en moet worden opgedwongen door de fabrikant. Daarom kiezen wij er voor deze firmware publiek te maken en deze keuze aan de consument te laten.

Huawei - B315s-22
The security of our products has the highest priority in Huawei. Upon receiving information on an issue, classified as 'low risk' by Agentschap Telecom, the Dutch Telecommunications Authority, Huawei has released a firmware upgrade for the router on September 2nd, effectively mitigating this risks.
We thank the researchers to report an unauthenticated information disclosure, before publication of the report which enabled Huawei to quickly address the issue and release a fix.

NETGEAR Nighthawk X4S R7800
The concerns identified by Agentschap Telecom require physical access (LAN connection) to the network and the router or proximity and knowledge of the secure WiFi network password. NETGEAR recommends customers use strong passwords and monitor connected devices to prevent unauthorized access.

NETGEAR DNS resolver is an internal query forwarder characteristic of the product design. It is not accessible to snoop remotely and thus should be of little concern to users and is not considered a security risk.

NETGEAR is committed to enhancing our product security, and is investigating certificates from Trusted Authorities that reduce browser warnings and encrypt credential transfer.

CONNECTED TOYS

Vtech Storio Max
VTech erkent het rapport over de Storio MAX en verwelkomt de bevestiging van Agentschap Telecom dat ´VTech voldoet aan de wettelijke vereisten met betrekking tot privacy´.
Wat betreft de vastgestelde kwesties:

- VTech neemt gegevensbescherming serieus en neemt passende maatregelen voor het beveiligen van gegevens.
- Gebruikers worden gevraagd om firmware-updates uit te voeren, indien beschikbaar.

- Om het kind eenvoudig toegang tot het apparaat te bieden, implementeren we geen kinderaccount-wachtwoord.
- Content van het kinderaccount is alleen zichtbaar op de tablet, niet op afstand.
- VTech zal zijn producten blijven verbeteren om te voldoen aan de verwachtingen van consumenten.

Makeblock Codeybot Wit
Makeblock Europe B.V. would like to respond to the report by the Telecom Agency. Makeblock takes the findings in this report with respect to its product the Codeybot to heart, although:

(i) this product has not been actively produced or sold by Makeblock since 2018; and
(ii) the privacy policy reviewed by the Telecom Agency is destined solely for the website and apps.

Makeblock wishes any customers of the Codeybot to be referred to a privacy policy addressing the Codeybot: https://www.makeblock.com/codeybot-privacy-policy. Please contact eu@makeblock.com or +31612645740 for any questions or concerns about the Codeybot or any other product by Makeblock.

Sphero Spider-Man Interactive App-Enabled Superhero
Our privacy policy was last updated on August 28, 2019. Sphero is willing to discuss this report with anyone interested in learning more about us and our privacy policies.

IP CAMERA'S

Hikvision DS-2CD2385FWD-I
Hikvision supports online device upgrades through client software, like Hik-Connect. Hikvision pushes the upgrade information to users timely. Hik-Connect account is not required for guest mode. Guest could operate if he can get and unlock the phone. We are evaluating to add the gesture or fingerprint authentication later. Hikvision cannot provide CA certificates for users, who need to acquire it by themselves (proving that they own the domain name), based on their decision on which domain name they will use. Hikvision has many product models, but data collection and processing is the same when using the products via Hik-Connect APP.

Foscam IP camera C1
Foscam is committed to provide safe products. Foscam Continuous improves products and will respond adequately to known threads. The intended communication with Foscam IP cameras is by using the Foscam APP or VMS-Software, both using encrypted communication. The Foscam APP informs if firmware updates are available. Upgrade is started by clicking the Upgrade button in the APP. The upgrade will be downloaded over a VPN-connection and installed automatically. All Foscam servers used comply with ISO-27018 (for Personal Data protection), CISPE, GDPR, EU-US privacy shield and Spanish DPA authorisation. Foscam started improvements to make sure users understand risks and their options.

SLIMME SLOTEN

Nuki Smart Lock
The Nuki Smart Lock is a retrofit product that can be mounted on a variety of different doors. In order to guarantee utmost security and convenience we provide extensive setting options in the App. We want to make it as easy as possible for users to adapt the Smart Lock to the individual needs and requirements. Thus, for example, the function of the button on the Smart Lock can be changed or disabled, just as the Bluetooth pairing and Auto-Unlock can be easily deactivated in the App's administration settings. We value privacy and ask customers only for data that is needed operate the service.

ASSA ABLOY - Nemef Entr
Veiligheid en beveiliging zit in ons DNA en we investeren uitgebreid in R&D / Innovatie om te waarborgen dat onze producten en oplossingen een veilige en gemakkelijke ervaring bieden. De SKG*** cilinder, 128-bits AES encryptie en de noodzaak om de knop in te drukken om te draaien, zijn enkele van de eigenschappen om de

ENTR te beveiligen. Dat gezegd hebbende, zullen we een optionele “ENTR knop houder” toevoegen aan nieuwe ENTR’s om te voorkomen dat de knop ingedrukt kan worden. Bestaande ENTR klanten kunnen met ons contact opnemen via 0900-4600460 om een gratis ENTR knop houder te ontvangen.

BABYFOONS

iBaby Monitor M6
iBaby Labs., Inc updated privacy policy to meet GDPR;
iBaby Labs., Inc updated terms and condition to meet GDPR;
iBaby Labs., Inc updated firmware to allow users to upgrade the app by themselves;
iBaby Labs., Inc updated apps to allow users to terminate their accounts;

SLIMME THERMOSTATEN

Google-Nest Learning Thermostat V3
Google Nest appreciates the report from the Dutch Radiocommunications Agency and the opportunity to comment. We are pleased that the Nest Learning Thermostat performed favorably in terms of both security and privacy and that there were no findings for Google Nest to address. Security and privacy are foundational to our products and to our brand, and we are always looking for opportunities to improve. Should the Agency have any suggestions for us, we would be happy to engage. Also, please make note of our new Privacy Commitments in the Home, announced at the last Google I/O, available here: https://store.google.com/nl/category/google_nest_privacy.

Bosch - Nefit ModuLine Easy
Wij zijn het eens met de genoemde bevindingen. Maar in geen enkel geval kan daardoor persoonlijke data worden achterhaald. Ook geeft dit geen veiligheidsrisico voor het verwarmingssysteem. Bij de “unencrypted REST API” gaat het slechts om algemene data zoals actuele links naar onze websites. De apps hebben momenteel geen “certificate pinning” maar de gegevens zijn wel degelijk versleuteld. Natuurlijk zijn wij van mening dat de communicatie state-of-the-art beveiligd hoort te zijn en hebben wij reeds releases ingepland met verbeteringen. De "DIGEST-MD5" -authenticatie, samen met aanvullende beveiligingsmaatregelen, blijft van kracht.