Nationales Testinstitut
für Cybersicherheit

Radio Equipment Directive (RED)

Rapport de synthèse sur la cybersécurité des appareils connectés au regard de la nouvelle directive RED

Version	1.0
Date	Jeudi 22 mai 2025
Classification	Public
Auteurs	Tobias Castagna, Patrik Fabian, Andreas Leisibach, Dilip Many, Raphael M. Reischuk, Fabio Zuber,
Responsable	Tobias Castagna

Sommaire

1 Management Summary

Le 1er août 2025, les nouvelles dispositions de la Radio Equipment Directive (RED) (2014/53/EU) entreront en vigueur en Suisse. Elles stipulent que les équipements radio doivent satisfaire à certaines exigences en matière de sécurité et de santé, notamment en ce qui concerne la cybersécurité des équipements connectés à Internet. Les exigences de la directive RED s'appliquent à presque tous les appareils dotés d'une interface radio. De nombreuses catégories de produits sont concernées, notamment les appareils IoT, les véhicules connectés, les applications de l'industrie 4.0 et les smartphones. Les appareils qui seront mis sur le marché à compter de l'entrée en vigueur de la directive RED doivent satisfaire à ces exigences. En cas de non-respect, l'OFCOM peut ordonner des mesures telles que des interdictions de commercialisation.

Le NTC a analysé un échantillon d'appareils connectés. Il s'agit de produits des catégories suivantes, fréquemment vendus dans le commerce suisse:

- Montres connectées pour enfants
- Babyphones avec caméra
- Systèmes d'alarme
- Adaptateurs de prises intelligents
- Routeurs WLAN

Les appareils ont été testés sur la base de certaines exigences de la directive RED, sélectionnées à titre d'exemple par le NTC. Il s'agit notamment des exigences suivantes, essentielles pour la sécurité et la résilience des appareils testés:

- Authentification et contrôle d'accès (p. ex. exigences relatives aux mots de passe par défaut)
- Communication protégée des données (procédé de cryptage moderne)
- Mises à jour sécurisées des logiciels (authenticité et intégrité des mises à jour)
- Protection contre la manipulation et les accès non autorisés (pas d'interfaces non sécurisées ou non documentées)

Principal résultat des échantillons NTC: un nombre important d'appareils contrôlés ne répond actuellement pas aux nouvelles exigences de la directive RED en matière de cybersécurité. Des exemples concrets illustrent la prévalence de ces failles: toutes les montres connectées pour enfants testées ainsi qu'un système d'alarme analysé présentaient un cryptage insuffisant dans la communication avec les plateformes cloud des fabricants concernés. Plusieurs babyphones avec caméra testés utilisaient des mots de passe par défaut non sécurisés. Par ailleurs, la transmission radio locale entre l'unité caméra et la station de base n'était pas suffisamment protégée contre l'écoute sur certains modèles. De plus, la majorité des routeurs WLAN et des adaptateurs de prises intelligents contrôlés n'utilisaient pas de cryptage ou seulement un cryptage insuffisant pour la communication, les informations sensibles telles que les mots de passe WLAN ou les paramètres du système pouvant être lues.

Le NTC préconise des mesures d'urgence sur toute la chaîne d'approvisionnement, des fabricants aux distributeurs en passant par les importateurs. Afin de se conformer à la réglementation prévue, il est recommandé aux fabricants de mettre en œuvre les exigences de manière proactive, aux importateurs et aux distributeurs d'exiger systématiquement des preuves de leurs fournisseurs et de sélectionner ces derniers avec soin. Les consommatrices et consommateurs peuvent eux aussi contribuer à leur sécurité en faisant leurs achats chez des distributeurs bien établis en Suisse, en faisant preuve de prudence lors d'importations directes, en changeant immédiatement les mots de passe par défaut et en installant régulièrement des mises à jour.