Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 26 janvier 2017
N° CERTFR-2016-ALE-009

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Campagne d'attaque contre des routeurs DSL

Gestion du document

Référence	CERTFR-2016-ALE-009
Titre	Campagne d'attaque contre des routeurs DSL
Date de la première version	01 décembre 2016
Date de la dernière version	26 janvier 2017
Source(s) heightPièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 - Risque(s)

– exécution de code arbitraire à distance

2 - Systèmes affectés

De nombreux routeurs vulnérables ont été victimes de cette attaque. Des systèmes vulnérables ont été rapportés outre en Allemagne, en Irlande, au Royaume-Uni, au Brésil ou encore en Finlande. Cette vulnérabilité dépend du matériel déployé par l'opérateur assurant l'accès à internet et la configuration qu'il a déployée sur celui-ci. L'attaque vise ici des routeurs dont la configuration expose le protocole TR-064 sur Internet au travers du port 7547.

Par ailleurs, plusieurs versions du binaire malveillant sont en circulation. Ces versions sont compilées pour s'exécuter sur différentes architectures (MIPS, ARM, SPARC). Cela montre la volonté des auteurs de cette attaque de toucher un large éventail d'équipements.

Il n'existe pas à ce jour de liste précise de systèmes affectés.

3 - Résumé

Le CERT-FR a constaté une importante campagne d'attaque à l'encontre de routeurs DSL. Ces routeurs mis à disposition par les fournisseurs d'accès internet pour leurs clients permettent la connexion à internet. Ils font l'objet d'une attaque d'une variante du ver Mirai visant à en prendre le contrôle et à les incorporer dans un réseau de machine zombie.

Cette vague d'attaque cible une vulnérabilité exploitable *via* le protocole TR-064 qui permet l'autoconfiguration du LAN (DHCP, SSDP, etc.). Ce service de configuration n'est en théorie accessible que depuis le réseau interne. Le protocole TR-069 est utilisé par les opérateurs pour administrer les routeurs à distance. Les équipements ciblés par cette attaque exposent un seul et même démon pour les protocoles TR-069 et TR-064. Dû à un défaut de cloisonnement réseau chez certains opérateurs, ces services sont accessibles depuis internet sur le port 7547. Cela à pour conséquence d'exposer le protocole TR-064 sur internet. Ce protocole présente une faille de sécurité permettant l'exécution de code à distance. Le code d'exploitation de la vulnérabilité a été publié dans un article de blog le 7 novembre 2016, et a été intégré au cadriciel d'exploitation publique Metasploit.

Une forte augmentation du trafic internet à destination du port 7547 a été observée à partir du 27 novembre et traduit des tentatives d'exploitation de la vulnérabilité.

La première phase de l'attaque consiste en l'envoi d'une requête SOAP émise à destination du port 7547 de l'équipement ciblé. La charge utile déclenche le téléchargement puis l'exécution d'un code malveillant disponible sur un serveur distant contrôlé par l'attaquant.

Le binaire téléchargé est une variante du ver Mirai qui s'attaquera au service d'administration du boitier accessible uniquement en local ou depuis le réseau interne du client. Une des premières opérations réalisées par Mirai consiste à supprimer le binaire du disque, il restera donc uniquement en mémoire et ne dispose d'aucun mécanisme de persistance. Le logiciel malveillant fermera également le port 7547 vulnérable. Il scannera ensuite internet à la recherche d'équipement présentant le port 7547 ouvert pour les infecter. Le déroulement de l'attaque des routeurs ne semble pas s'être déroulé correctement sur les équipements de l'opérateur allemand Deutsche Telekom provoquant une interruption de l'accès à internet de centaines de milliers de clients entre dimanche 27 et lundi 28 novembre 2016.

4 - Solution

Pour les opérateurs, il est recommandé de restreindre l'accès aux interfaces d'administration depuis un réseau dédié, exclusivement accessible par l'opérateur et authentifié.

Enfin, le code malveillant s'exécutant en mémoire, un redémarrage de l'équipement permet d'éliminer le ver. Cependant tant que le ver continue à se propager et que la vulnérabilité n'est pas corrigée par l'opérateur, le routeur sera rapidement réinfecté.

5 - Documentation

- Article de Flashpoint sur les répercussions de l'attaque en Allemagne
  https://www.flashpoint-intel.com/new-mirai-variant-involved-latest-deutsche-telekom-outage/
- Article de BadCyber sur la vulnérabilité exploité dans l'attaque
  https://badcyber.com/new-mirai-attack-vector-bot-exploits-a-recently-discovered-router-vulnerability/
- Article de Securelist sur la vulnérabilité exploité dans l'attaque
  https://securelist.com/blog/incidents/76791/new-wave-of-mirai-attacking-home-routers/
- Message sur le forum SANS ISC détaillant la vulnérabilité sur le protocole TR-069
  https://isc.sans.edu/forums/diary/TR069+NewNTPServer+Exploits+What+we+know+so+far/21763/1
- Article original annonçant la vulnérabilité sur le protocole TR-069
  https://devicereversing.wordpress.com/2016/11/07/eirs-d1000-modem-is-wide-open-to-being-hacked/
- Communiqué de presse de Deutsche Telekom concernant l'attaque sur leus équipements
  https://www.telekom.com/en/media/details/the-open-interface-myth-445290

Gestion détaillée du document

01 décembre 2016 version initiale.
05 décembre 2016 correction sur les détails de la campagne.
26 janvier 2017 clôture de l'alerte.