Bonjour et bienvenue sur No Limites Sécu, le podcast francophone hebdomadaire dédié à la cyber-sécurité.
Alors aujourd'hui nous allons parler d'une vulnérabilité qui impacte un grand nombre de routers avec Patrice Aufret. Bonjour Patrice.
Bonjour.
Pour discuter avec lui, les contributeurs No Limites Sécu sont Vladimir Collin.
Bonjour.
Hervé Chauheur.
Bonjour.
Et Nicolas Ruff.
Bonjour.
Alors Patrice, on a déjà réalisé un épisode ensemble sur Onif, mais pour les auditeurs qui ne l'auraient pas suivi, est-ce que tu voudrais bien te présenter ?
Tout à fait. Je m'appelle Patrice Aufret. J'ai créé la société Onif en 2017 et on évolue dans le domaine de la découverte de la surface d'attaque. Et pour ce faire, on scanne toute Internet, IPv4, IPv6, mais également des URL. C'est très important de scanner des URL puisque si on a des adresses IP derrière Clou de Flair par exemple, si on scanne que l'adresse IP, on verra pas les technologies des sites web protégés.
Alors Patrice, comment cette vulnérabilité a été découverte ?
Alors c'est l'équipe de Cisco Talos qui, sur une investigation, à la demande d'un client, s'est rendu compte qu'il y avait des comptes admin, donc c'est privilège 15 du côté de Cisco, l'équivalent de route sur une X. Des comptes étaient créés à distance et du coup ils ont investigué pour savoir comment c'était possible que des comptes administrateurs soient créés à distance comme ça.
Et par quelle magie s'arrivait ? Et par quelle magie, ils ont continué leur investigation et ils se sont rendu compte qu'une faille de type 0D était exploitée.
Ils ont continué à investiguer, ils se sont rendu compte que le phénomène était assez prévalent et un certain nombre d'acteurs ont commencé à scanner Internet pour regarder jusqu'à quel point c'était grave puisque Talos, dans sa grande générosité, a donné une méthode d'identification à distance pour savoir si une machine avait un implant ou pas, puisqu'il faut le rappeler, cette vulnérabilité était exploitée pour déployer des implants, donc prendre le contrôle total de routeurs à l'échelle d'Internet.
Oui, alors ce qu'on peut dire c'est que c'est une vulnérabilité qui à distance permet de créer un compte, donc une vulnérabilité ultra critique et qui a été exploitée par un attaquant, on ne sait pas qui, et ce qu'a communiqué Talos c'est effectivement un moyen de détecter certains implants, en tout cas les premiers implants que eux ont découvert, malheureusement comme il y a eu beaucoup de codes d'exploitation et autres qui ont été publiés depuis, ça ne permet pas de potentiellement de détecter tous les implants qui ont été créés depuis, mais au moins ça permet de détecter tous ceux du passé, c'est à dire qu'il y a quand même quelqu'un, des gens qui ont compromis des milliers, voire dizaines de milliers, on en reparlera, mais d'équipements Cisco et pour injecter des comptes. Donc il y a des gens qui ont utilisé cette capacité de création de compte administrateur pour injecter un implant, c'est à dire du code à l'intérieur du routeur ?
C'est ça. Oui, tout à fait. Ce qu'il faut savoir c'est qu'au tout début, alors comment ça a

commencé ? En fait, Talos a investigué sur cette affaire, c'était fin septembre à peu près, donc il a constaté un certain nombre de routeurs, mais en petit nombre, et à peu près deux, trois semaines plus tard, l'attaque a été lancée à large échelle et pour la plupart des routeurs compromis d'après la naïse de Cisco, ce serait l'œuvre d'un acteur unique. Alors depuis, comme Vlad l'a dit, la vulnérabilité est connue, donc il y a d'autres acteurs certainement qui s'engouffrent
dans la brèche, mais l'essentiel des machines compromises aujourd'hui est attribué à un unique acteur.
Mais il y a une fuite chez Talos, alors parce que si cet acteur s'est mis à utiliser la faille de manière très générale juste après sa découverte par Talos, soit il s'est aperçu que ça avait été découvert, soit il y a une fuite de chez Talos. Bah non, pas forcément, ça peut être au contraire, l'inverse, c'est que le client de Talos est suffisamment réactif pour avoir détecté ça
au tout début, au prémis, et qui sont juste arrivés au tout début de la campagne de l'attaquant, et que c'est juste l'attaquant, il avait prévu ensuite d'exploiter massivement sa vulnérabilité, c'est peut-être juste ça. C'est ça, en fait, les fins septembre, on peut attribuer ça à des tests, pour voir en gros si la procédure automatique d'attaque en masse allait bien fonctionner, et c'est là qu'ils ont été repérés. C'est triste pour eux, ils ont été pris la main dans le pot de confiture, c'est dommage, enfin dommage. Exactement, ce qui amène à la question suivante, quel était l'objectif, puisque aujourd'hui, à ma connaissance, il n'y a pas eu de demande de renseau sur les équipements concernés, donc quel était l'attaquant ? C'est de l'espionnage ou du prépositionnement stratégique évidemment, on ne va pas consommer un 0D pour du renseau Surtout que si on parle en termes de machines compromises, d'après nos données, il y a 80 000 équipements exposés à internet, nous on a constaté 53 000 équipements compromis, donc quand on fait
une attaque à si grande échelle, c'est un peu difficile d'imaginer que ça va passer inaperçu, donc ça pose aussi tout un tas de questions. Ah tu penses que ça peut pas passer inaperçu, ça peut être comme si c'est assez fin, assez discret, tu n'aisses pas trop de traces, trop de logs, ça n'est finalement qu'une ou deux requêtes sur chaque cible. Oui mais ça s'est fait en l'espace de 24 heures en gros. Oui ça effectivement. Il y a d'autres acteurs comme Shadow Server ou Leakix ou Senseis qui ont également scanner les équipements pour identifier ceux qui lui avaient l'implant. Senseis par exemple a constaté une augmentation de 8 000 machines compromises en l'espace de 8 heures, je pense qu'ils ont amélioré leur procès de détection puisqu'on avait déjà 53 000 avant leur second scan mais ce qui est certain c'est que ça s'est passé sur un temps court cette compromission à de dizaines de milliers de routers à l'arge échelle. Et est-ce qu'il y a une typologie spécifique d'un vertical ou plusieurs qui ont été ciblés ? Je pense que c'est vraiment tout ce qui était exposé à internet, dans nos données on a constaté qu'il y en avait en Chine également qui était impacté en Russie aussi si on cite que c'est deux pays là mais en gros c'est vraiment tous les équipements quel que soit le pays qui ont été ciblés et moi je dirais qu'on peut considérer aujourd'hui que tous ceux qui sont exposés sont compromis. La différence pourquoi on arrive à 53 000 et pas 80 000 sur 80 000 c'est qu'il est possible que l'implant soit pas vraiment bien installé puisque ça nécessite un redémarrage du processus web et aussi bien dans l'outil automatique il y a eu un bug et c'est pas arrivé jusqu'au redémarrage pour vraiment déployer l'implant mais moi je considère aujourd'hui que tous ces routers là sont compromis. Par contre

sur les cibles il y a quand même une grande partie des cibles qui sont américaines c'est que c'est 15% enfin c'est très américain du nord et américain du sud c'est-à-dire dans les plus pirataires il y a les américains, philippines, mexicaux, chili, indes, alliés quand même des Etats-Unis, Thaïlande, Australie, Singapour, Brésil, Angleterre, Equateur et Pologne. Donc en fait ça c'est la liste des principaux piratés c'est quand même très très orienté alliance nord-américaine.
Oui si on regarde nos données sur les 53 000 compromis il y en a 10 000 aux us c'est vraiment le numéro 1 de loin. Après Cisco c'est un éditeur américain donc il est aussi très déployé aux Etats-Unis.
Oui mais est-ce qu'il n'y a pas des rebonds ? Est-ce qu'il n'y a pas des dizaines de milliers de routeurs qui ne sont pas visibles sur internet dans des réseaux privés, qui n'auraient pas été aussi compromis que tu ne peux pas voir avec Onif ? Non parce que ce qu'on n'a pas dit c'est que pour
exploiter la faim il faut se connecter à l'interface web publique du routeur donc il faut avoir exposé son interface d'administration web sur internet pour être une erapeciton-routeur à une récit privé qui est à l'intérieur d'un réseau. S'il a été compromis c'est que l'attaquant est déjà quelque part sur ton réseau interne et qu'il a accès en direct aux interfaces d'administration. Je crois que c'est le millième fois qu'on le dit mais n'exposer jamais un portail d'administration de ce genre d'équipement sur internet. Oui c'est vrai qu'on a oublié de dire qu'effectivement ça impacte le composant web du routeur Cisco. La recommandation de Cisco c'est de
désactiver l'interface web tout simplement pour éviter d'être compromis. Moi je dirais que tous ceux qui ont ce type d'équipement aujourd'hui doivent faire une analyse informatique puisque comme je le disais je considère qu'ils sont tous compromis donc il ne suffit pas de tester est-ce que l'implant est sur mon routeur ou pas non faut faire une analyse informatique parce qu'il y a 90% de chance qu'il soit compromis. Oui totalement oui. Nous c'est ce qu'on recommande à nos clients c'est même si vous n'avez l'impression que vous n'êtes pas compromis il faut impérativement investiguer parce que entre potentiellement les bugs du premier implant et les évolutions d'autres implants d'autres attaquants c'est très compliqué donc il faut impérativement investiguer. Et investiguer ça veut dire regarder. Je suis désolé c'est arrivé en pleine semaine on arrive sur le week-end c'est très très compliqué mais c'est malheureusement il faut le faire. Oui alors investiguer Cisco Talos a donné aussi les AY aussi pour identifier une compromission des routeurs il y a une méthode simple si il y a un fichier qui s'appelle de mémoire Cisco underscore services.conf dans l'arborécence ça veut dire que l'implant a été déployé enfin l'implant l'implant découvert par Cisco Talos et Vlad voilà il y a peut-être d'autres implants donc d'autres AY aussi
à aller regarder. C'est à dire qu'il faut quand même regarder la liste des comptes des utilisateurs à minima voir si un compte inconnus n'ont maîtrisé et fait attention parce que Admin avec deux N enfin N à la place du M etc il y a des astuces qui permettent de cacher visuellement vérifier quand même tous les noms des comptes. Oui et quand il y a un compte de créé il y a une ligne qui est
journalisée dans l'équipement donc il suffit de regarder est-ce qu'il y a des comptes qui ont été créés récemment et de regarder est-ce que c'est normal. Si vous êtes suffisant en matière pour sortir vos logs et les centraliser dans un cm ou autre vous regardez tous les comptes qu'ont

été créés depuis on va dire quelques semaines et ça vous permettra quand même d'avoir des indices sur la compromission potentielle de l'équipement. Dico tu voulais réagir ? Oui je voulais réagir à quelque chose qu'on a dit de tout à l'heure sur le fait que les attaquants étaient extrêmement verbeux et avaient compromis en masse plein de routeurs pour moi c'est une stratégie payante parce que quand tu regardes certaines failles qui a pu avoir dans le passé dans exchange ou des firewalls des gateway VPN et tout comme ça un an après tu as encore 70% des gens compromis qui
n'ont pas nettoyé donc en fait même si aujourd'hui il y a des publications Cisco Talos il y a des alertes CISA certes FR etc tu peux être certain que dans 6 mois la majorité des implants sera encore installé sur ces routeurs. Exactement et ça c'est ce qui m'intéresse d'un point de vue chercheur on va dire. Nous on va monitorer ça toutes les semaines en gros on va regarder où sont les implants donc on aura des chiffres sur l'évolution de cette attaque et je suis convaincu
comme toi Nico que dans 6 mois on verra encore des machines avec un implant. Alors ce qu'il faut savoir c'est qu'il ne survie pas en reboute donc si on voit encore des machines dans 6 mois avec l'implant c'est qu'elles n'ont pas rebouté bon il y a le droit de pas rebouter son serveur mais c'est ça qui va être intéressant pour moi d'un point de vue chercheur. Si elle ne survit pas au reboute mais si un utilisateur donc route qui a été créé sera toujours là. Exactement exactement et c'est pour ça qu'il faut vraiment ne pas se baser uniquement sur la présence de l'implant pour établir l'état compromis ou non compromis de son équipement. Le problème du reboute c'est que c'est pas non plus anodin parce que c'est quand même des routers sur une certaine taille qui font passer pas mal le trafic et leur démarrer déjà ça prend un certain temps et donc si en plus
il n'y a pas de redondance si vous avez de la redondance vous pouvez faire d'abord le master ensuite le slave mais si vous n'avez pas de redondance ça peut occasionner une coupeur de service assez importante. On peut comprendre que les gens n'aient pas envie de rebouter tout de suite
ça peut aussi se comprendre. Bien sûr et on sait que les opérationnels n'aiment pas redémarrer les serveurs puisqu'il y a toujours des risques même au niveau pas de matériel mais la situation est suffisamment grave pour trouver une fenêtre d'intervention je pense. Oui totalement. Est-ce qu'il n'est pas possible de poser des implants persistants parce qu'il y a quand même des mémoires. Enfin je
pourrais flasher le firmware sur ces équipements donc il me semble que par les passés il y a eu des cas où des routers avaient pu être compromis de manière persistante et je ne te parle même pas des gens qui compromet des routers dans la supply chaine c'est à dire qu'ils ouvrent les colis avant qu'ils arrivent chez toi et qu'ils reflâchent un firmware backdoré dans l'équipement. Est-ce qu'on peut garantir l'inocuité d'un équipement de matériel si on a réinstallé une version d'IOS 6xIOS 2. Clairement non surtout que les comptes sont admins donc ils peuvent vraiment modifier la conf qui est enregistrée en mémoire et donc qui persiste reboute donc non c'est pour ça qu'il faut enquêter donc il faut enquêter c'est vraiment l'essentiel. Oui mais même enquêter enfin les recommandations qui existaient à quelques années c'est si un équipement est compromis il faut le réinstaller complètement, installer les patchs et ensuite le connecteur réseau. Cette recommandation
ça fait longtemps que je ne l'ai pas entendu mais pour ce genre de vulnérabilité je pense que la meilleure solution c'est vraiment de reflâcher le device, le patcher avant de le connecter de nouveau au réseau et ensuite seulement de reconnaitre au réseau. Après il y a le problème de la

configuration, c'est à dire que tu as toute ta configuration au réseau, tes comptes etc qu'il faut également remettre dans l'équipement mais il faut quand même l'analyser pour être sûr qu'il n'y a pas un compte encore une fois porte dérobé qui aurait été ajouté. Tout à fait c'est pas simple. C'est pour ça qu'on le fait de moins en moins faire un reset complet d'un système parce que c'est devenu compliqué surtout des équipements presque le coeur de réseau j'ai envie de dire c'est compliqué d'avoir cette approche. C'est vraiment pas un cadeau là je plains toutes les équipes réseaux qui se prennent ça là c'est pas un sujet facile à traiter.
Une des attaques qu'elle faisait référence par exemple est connu ce nom du groupe Tangri 4 qui avait quand même réussi à analyser le bitstream du FPGA qui est dans les équipements Cisco pour assurer l'authenticité et en modifiant ce bitstream depuis un chale route il pouvait bypasser en fait la vérification intégrité des firmwares et pourquoi ? Parce qu'en fait aujourd'hui il y a énormément d'équipements contrefait aussi donc le contournement de tous ces devices de sécurité et de DRM côté vendeur et aussi un sujet de recherche pour tous les fabricants de clones bascou et bascualité. Moi ce que j'ai du mal à comprendre c'est qu'est-ce qui peut justifier d'exposer l'interface d'administration ou web d'un router sur internet ? Rien, rien, je le fais jamais, vos firewalls, vos routers, vos proxies, n'exposez pas les interfaces d'administration, même vos
WordPress, vos CMS, n'exposez pas les interfaces d'administration de ça sur internet. Il y en a 53 000 qui l'ont fait donc... Ce qui est le problème c'est qu'après c'est souvent des routers de tête de réseau qui sont vraiment en frontale d'internet donc peut-être que c'est une mauvaise configuration, un manque de durcissement, alors je vais pas laiser les confs. C'est juste une mauvaise
installe par défaut. Peut-être, je pense pas que c'est sûr aussi volontaire. Moi je croyais qu'il fallait lancer la commande pour que l'interface d'administration soit web soit lancée en fait à des par défauts.
J'en sais rien et puis surtout je me semble que les par défaut et pour lancer la commande pour la désactivation. Potentiellement il faudrait une interface d'admins sur un réseau privé mais si les routers ils sont adressés que sur du public, avoir un réseau d'admins déconnecté du réseau public c'est quand même pas évident donc tu peux comprendre que les mecs laissent la interface d'admins sur une IP publique auxquels ils accèdent mais vraiment ne le faites pas. Essayez vraiment d'avoir des liens dédiés des réseaux d'admins déconnectés et pas du tout reliés à internet.
Ce qu'il faut bien voir c'est que c'est toujours la même histoire. Un fabricant de produit, il livre un produit et il faut qu'il soit utilisable le plus rapidement possible sans avoir à rentrer dans la doc pour réussir à l'administrer. Donc souvent c'est ce dispositif de type routers, l'interface web elle écoute par défaut pour qu'on puisse se connecter avec le mois de passe par défaut et configurer la machine pour que ça marche et le guide de hardeaning il est souvent de manquant dans les équipements mais effectivement il y a l'étape finale une fois que ça marche le hardeaning et ça souvent les utilisateurs ils sont laissés eux-mêmes sur ces aspects là.
Parce que c'est un gros travail en amont. Normalement il faut que tu aies des templates de conf qui soient validés, que tu aies des standards qui soient ensuite appliqués sur tous tes équipements et industrialisés, ça demande quand même un gros travail en amont.
Ok donc quelles sont les actions qu'on peut recommander de mettre en œuvre dès que possible. Contre les utilisateurs, désactiver l'interface web, rebooter, patcher. Est-ce qu'il y a un patch qui est disponible ? Au dernière nouvelle je n'ai pas vu je sais que Cisco travaillait d'arrache pied

pour fournir un patch je trouve ça un petit peu long et bon on ne connaît pas les procès de Cisco. Au moment de l'enregistrement de cet épisode aucun correctif de sécurité n'est encore disponible. Et Cisco a un petit peu rationalisé ses lignes de produits mais il faut voir qu'à une époque il y avait des builds de routeurs qui étaient faits par clients c'est-à-dire que quand tu avais un support ingénieur de plus haut niveau qui venait chez toi et que tu avais un bug il te recompilait du Cisco IOS sur sa machine et il te déployait sur ton routeur donc à un moment quand tu avais un compte, je ne sais pas comment c'est à nous là, tu pouvais télécharger jusqu'à 300 000 firmwares différents donc t'imagines qu'en termes de QA, de recompilation, de test etc c'est vraiment l'enfer. Oui je ne suis pas surpris j'ai travaillé pour un grand fabricant de modem câble DSL et à l'époque on avait quelque chose comme 400 branches software parce que c'était du custom par client quasiment donc ça complexifient un peu le portage du bug fixe sur toutes les branches
software. Donc oui les recommandations aujourd'hui c'est numéro un désactiver l'interface web et idéalement le déconnecter du réseau pour faire une investigation pour savoir si deva il s'est compromis ou pas. Alors il y a eu des nouveautés depuis le moment où nous avons enregistré cet épisode. Alors Patrice, quels sont ces nouveautés ? Il y a deux grandes nouveautés effectivement. La première nous vient de Cisco Talos. Finalement c'est bien une chaîne de vulnérabilité qui a été exploité et ce n'est pas une 0d mais deux. La première on l'a vu c'est celle permettant d'un création d'un compte administrateur sur l'équipement et la seconde serait une escalade de privilèges locales pour atteindre les droits routes et pouvoir déployer l'implant au niveau du système. La deuxième grande nouveauté c'est que nous avons constaté que les implants disparaissaient
d'internet. Ça ne veut pas dire que les devas n'ont pas été compromis. Ça peut dire tout simplement que l'attaquant est en train de nettoyer ses traces puisque cette méthode de détection à distance n'aurait peut-être pas dû être possible en premier lieu donc ils sont en train de corriger leur erreur ou alors ça veut dire éventuellement que quelqu'un est en train de nettoyer les implants à large échelle. Pour l'instant nous n'en savons pas plus. De mon côté je continue à penser qu'il faut considérer que tous les équipements donc les 80 000 équipements sont compromis et je ne
peux qu'inviter les administrateurs de ces équipements à effectuer une analyse informatique pour s'assurer
que leur équipement n'a pas été compromis. Ok est ce que vous voyez d'autres choses à ajouter ? Bon je pense que de mon côté c'est bon. Nous on va continuer à monitorer pour savoir si l'attaque se répand un peu plus ou si les implants restent en ligne longtemps ou pas. Et tu vas continuer à publier sur Twitter ce que tu trouves ? Tout à fait oui. Cool alors et ton compte Twitter c'est ?
Bon et bien Patrice merci beaucoup d'avoir accepté notre invitation. Merci aux contributeurs. Chers auditeurs nous espérons que cet épisode vous aura intéressé et nous vous dénons. Rendez-vous la semaine prochaine pour un nouveau podcast. Au revoir.
Sous-titres réalisés par l'Amara.org