Groupe de travail Réseau
Request for Comments : 4272
Catégorie : Information
Traduction Claude Brière de L'Isle

S. Murphy, Sparta, Inc.

janvier 2006

Analyse des vulnérabilités de la sécurité de BGP

Statut de ce mémoire
Le présent document fournit des informations pour la communauté de l'Internet. Il ne spécifie aucune sorte de norme de l'Internet. La distribution du présent mémoire n'est soumise à aucune restriction.

Résumé
Le protocole de routeur frontière 4 (BGP-4, *Border Gateway Protocol 4*) avec un hôte d'un autre protocole d'infrastructure connu avant que l'environnement de l'Internet devienne périlleux, a été à l'origine conçu sans considération de la protection des informations qu'il porte. Il n'y a pas de mécanisme interne à BGP qui protège contre les attaques qui modifient, suppriment, falsifient, ou répètent les données, qui ont toutes le potentiel de perturber le comportement global d'acheminement du réseau.

Le présent document discute certaines des questions de sécurité de la dissémination des informations d'acheminement de BGP. Le présent document ne discute pas les questions de sécurité de la transmissions des paquets.

Table des matières

1. Introduction

Le protocole d'acheminement inter domaines BGP a été créé quand l'environnement de l'Internet n'avait pas encore atteint l'état de conflit présent. Par conséquent, la conception de BGP n'incluait pas de protection contre les erreurs délibérées ou accidentelles qui pouvaient causer des perturbations du comportement d'acheminement.

Le présent document discute des vulnérabilités de BGP, sur la base de la spécification de BGP [RFC4271]. Les lecteurs sont supposés familiarisés avec la RFC de BGP et le comportement de BGP.

Il est clair que l'Internet est vulnérable à l'attaque à travers ses protocoles d'acheminement et BGP n'y fait pas exception. Des sources fautives, mal configurées, ou délibérément malveillantes peuvent perturber le comportement global de l'Internet en injectant des informations d'acheminement boguées dans la base de données d'acheminement distribuée par BGP (en modifiant, falsifiant, ou répétant des paquets BGP). Les mêmes méthodes peuvent aussi être utilisées pour perturber le comportement du réseau local et global en cassant la communication distribuée des informations entre homologues BGP. Les sources des informations boguées peuvent être des extérieurs ou de vrais homologues BGP.

L'authentification cryptographique de la communication entre les homologues ne fait pas partie intégrante de BGP. En tant que protocole TCP/IP, BGP est sujet à toutes les attaques TCP/IP, par exemple, l'usurpation d'identité IP, le vol de session, etc. Tout extérieur peut injecter des messages BGP crédibles dans la communication entre homologues BGP, et par là injecter des informations d'acheminement boguées ou casser la connexion entre les homologues. Toute coupure dans la communication entre les homologues a un effet d'ondulation d'acheminement qui peut être largement étendu. De plus, des sources extérieures peuvent aussi interrompre les communications entre homologues BGP en cassant leur connexion TCP avec des paquets falsifiés. Les sources externes d'informations BGP boguées peuvent résider n'importe où dans le monde.

Par conséquent, la spécification BGP actuelle exige qu'une mise en œuvre de BGP prenne en charge le mécanisme d'authentification spécifié dans la [RFC2385]. Cependant, l'exigence de prise en charge de ce mécanisme d'authentification ne peut pas assurer que le mécanisme soit configuré à être utilisé. Le mécanisme TCP MD5 de la [RFC2385] se fonde sur un secret partagé préinstallé ; il n'a pas la capacité d'IPsec [RFC2401] de s'accorder de façon dynamique sur un secret partagé. Par conséquent, l'utilisation de la [RFC2385] doit être une décision délibérée, et non une caractéristique automatique ou par défaut.

La spécification BGP actuelle permet aussi des mises en œuvre qui accepteraient des connexions avec des "homologues non configurés" ([RFC4271] Section 8). Cependant, la spécification n'est pas claire sur ce que pourrait être un homologue non configuré, ou sur comment les protections de la [RFC2385] s'appliqueraient dans un tel cas. Donc, il n'est pas possible d'inclure une analyse des questions de sécurité de cette caractéristique. Quand une spécification qui décrira plus complètement cette caractéristique sera publiée, une analyse de la sécurité devrait faire partie de cette spécification.

Les locuteurs BGP eux-mêmes peuvent injecter des informations d'acheminement boguées, soit en se faisant passer pour un autre locuteur BGP légitime, soit en distribuant par eux-mêmes des informations d'acheminement non autorisées. Historiquement, des routeurs mal configurés et fautifs ont été responsables de grandes interruptions dans l'Internet. Les homologues BGP légitimes ont le contexte et les informations pour produire des informations d'acheminement crédibles, bien que boguées, et ont donc l'opportunité de causer de gros dommages. Les protections cryptographiques de la [RFC2385] et les protections opérationnelles ne peuvent pas exclure que des informations boguées proviennent d'un homologue légitime. Le risque d'interruptions causées par des locuteurs BGP légitimes est réel et ne peut pas être ignoré.

Des informations d'acheminement boguées peuvent avoir de nombreux effets différents sur le comportement d'acheminement. Si les informations boguées suppriment des informations d'acheminement pour un certain réseau, ce réseau peut devenir inaccessible pour la portion de l'Internet qui accepte les informations boguées. Si les informations boguées changent la route pour un réseau, les paquets destinés à ce réseau peuvent alors être transmis par un chemin sous optimal, ou par un chemin qui ne suit pas la politique attendue, ou par un chemin qui ne va pas transmettre le trafic. Par conséquent, le trafic pour ce réseau pourrait être retardé par un chemin plus long que nécessaire. Le réseau pourrait devenir inaccessible à partir de zones où les informations boguées sont acceptées. Le trafic peut aussi être transmis le long d'un chemin qui permet à des adversaires de voir ou modifier les données. Si les informations boguées font apparaître qu'un système autonome est à l'origine d'un réseau alors qu'il ne l'est pas, les paquets pour ce réseau peuvent n'être pas livrables pour la portion de l'Internet qui accepte les informations boguées. Une fausse annonce qu'un système autonome est à l'origine d'un réseau peut aussi fragmenter des blocs d'adresses agrégées dans d'autres parties de l'Internet et causer des problèmes d'acheminement pour les autres réseaux.

Les dommages qui peuvent résulter de ces attaques incluent :

famine : le trafic de données destiné à un nœud est transmis à une partie du réseau qui ne peut pas le livrer.

encombrement du réseau : plus de trafic de données est transmis à travers une portion du réseau qui n'aurait autrement pas besoin de porter le trafic.

trou noir : de grandes quantités de trafic sont dirigées pour être transmises à travers un routeur qui ne peut pas traiter le niveau accru de trafic et abandonne beaucoup, la plupart, ou tous les paquets.

retard : le trafic de données destiné à un nœud est transmis le long d'un chemin qui est d'une certaine façon inférieur au chemin qu'il aurait pris autrement.

boucle : le trafic de données est transmis le long d'un chemin qui fait une boucle, de sorte que les données ne sont jamais livrées.

espionnage : le trafic de données est transmis à travers un routeur ou réseau qui ne verrait autrement pas le trafic, offrant une opportunité de voir les données.

partition : certaines portions de réseau croient qu'elles sont séparées du reste du réseau, alors qu'en fait, elles ne le sont pas.

coupure : certaines portions de réseau croient qu'elles n'ont pas de route pour un réseau auquel elles sont en fait connectées.

bouillonnement : la transmission dans le réseau change à un rythme rapide, résultant en grandes variations du schéma de livraison des données (et affectant les techniques de contrôle d'encombrement).

instabilité : BGP devient instable d'une façon telle que la convergence sur l'état global de transmission n'est pas réalisée.

surcharge : les messages BGP eux-mêmes deviennent une portion significative du trafic que porte le réseau.

épuisement de ressources : les messages BGP eux-mêmes causent l'épuisement de ressources critiques de routeur, comme l'espace de tableau.

usurpation d'adresse : le trafic de données est transmis à travers un routeur ou réseau qui usurpe une adresse légitime, permettant ainsi une attaque active en offrant l'opportunité de modifier les données.

Ces conséquences peuvent tomber exclusivement sur un préfixe de système d'extrémité ou peuvent affecter le fonctionnement du réseau tout entier.

1.1 Spécification des exigences

Les mots clés "DOIT", "NE DOIT PAS", "EXIGE", "DEVRA", "NE DEVRA PAS", "DEVRAIT", "NE DEVRAIT PAS", "RECOMMANDE", "PEUT", et "FACULTATIF" en majuscules dans ce document sont à interpréter comme décrit dans le BCP 14, [RFC2119].

2. Attaques

BGP est par lui-même sujet aux attaques suivantes. (La liste est tirée de la RFC de l'IAB qui fournit des lignes directrices pour la Section "Considérations sur la sécurité" des RFC [RFC3552].)

violations de la confidentialité : les données d'acheminement portées dans BGP sont en clair, de sorte que l'espionnage est une attaque possible contre la confidentialité des données d'acheminement. (La confidentialité des données d'acheminement n'est pas une exigence courante.)

répétition : BGP ne fournit pas de protection contre la répétition de ses messages.

insertion de message : BGP ne fournit pas de protection contre l'insertion de messages. Cependant, comme BGP utilise TCP, quand la connexion est pleinement établie, l'insertion de message par un extérieur exigerait une prédiction précise du numéro de séquence (non entièrement hors sujet, mais plus difficile avec des mises en œuvre plus mûres de TCP) ou des attaques de vol de session.

suppression de message : BGP ne fournit pas de protection contre la suppression des messages. Là encore, cette attaque est plus difficile contre une mise en œuvre expérimentée de TCP, mais elle n'est pas entièrement hors propos.

modification de message : BGP ne fournit pas de protection contre la modification des messages. Une modification qui est syntaxiquement correcte et ne change pas la longueur de la charge utile TCP ne sera en général pas détectable.

interposition : BGP ne fournit pas de protection contre les attaques par interposition. Comme BGP n'effectue pas l'authentification de l'entité homologue, une attaque par interposition est un jeu d'enfant.

déni de service (DoS) : bien que les données d'acheminement boguées puissent présenter un risque d'attaque de déni de service sur les systèmes d'extrémité qui essayent de transmettre des données à travers le réseau et sur l'infrastructure de réseau elle-même, certaines informations boguées peuvent représenter un potentiel de déni de service sur le protocole d'acheminement BGP. Par exemple, annoncer un grand nombre de routes plus spécifiques (c'est-à-dire, des préfixes plus longs) peut causer l'augmentation du trafic BGP et de la taille des tableaux de routeur, jusqu'à les faire exploser.

Le mécanisme de mise en œuvre obligatoire de la [RFC2385] va contrer les attaques d'insertion, suppression, et modification de messages, d'interposition et de déni de service provenant de l'extérieur. L'utilisation de la [RFC2385] ne protège pas contre les attaques d'espionnage, mais la confidentialité des données d'acheminement n'est pas un objectif pour BGP. Le mécanisme de TCP MD5 ne protège pas contre les attaques en répétition, de sorte que la seule protection contre la répétition est fournie par le traitement du numéro de séquence de TCP. Donc, une attaque en répétition pourrait être montée

contre une connexion BGP protégée par TCP MD5 mais seulement dans ces circonstances. Le mécanisme de la [RFC2385] ne peut pas protéger contre les informations d'acheminement boguées générées de l'intérieur.

3. Vulnérabilités et risques

Les risques dans BGP proviennent de trois vulnérabilités fondamentales :

(1) BGP n'a pas de mécanisme interne qui fournisse une protection forte de l'intégrité, de la fraîcheur, et de l'authenticité des messages de l'entité homologue dans les communications BGP d'homologue à homologue.

(2) Aucun mécanisme n'a été spécifié dans BGP pour valider l'autorité d'un AS pour annoncer les NLRI.

(3) Aucun mécanisme n'a été spécifié dans BGP pour assurer l'authenticité des attributs de chemin annoncés par un AS.

La première vulnérabilité fondamentale a motivé la prise en charge obligatoire de la [RFC2385] dans la spécification BGP. Quand la prise en charge de TCP MD5 est employée, l'intégrité du message et l'authentification de l'entité homologue sont fournies. Le mécanisme de la [RFC2385] suppose que l'algorithme MD5 est sûr et que le secret partagé est protégé et choisi comme difficile à deviner.

Dans la discussion qui suit, les vulnérabilités sont décrites dans les termes des événements de l'automate à états finis de BGP. Les événements sont définis et discutés à la Section 8 de la [RFC4271]. Les événements mentionnés ici sont :

[Événements administratifs]
Événement 2 : ManualStop *(arrêt manuel)*
Événement 8 : AutomaticStop *(arrêt automatique)*

[Événements de temporisateur]
Événement 9 : ConnectRetryTimer_Expires *(expiration du temporisateur d'essais de connexion)*
Événement 10 : HoldTimer_Expires *(expiration du temporisateur de garde)*
Événement 11 : KeepaliveTimer_Expires *(expiration du temporisateur de garde en vie)*
Événement 12 : DelayOpenTimer_Expires *(expiration du temporisateur de retard d'ouverture)*
Événement 13 : IdleHoldTimer_Expires *(expiration du temporisateur de garde en repos)*

[Événements fondés sur la connexion TCP]
Événement 14 : TcpConnection_Valid *(connexion TCP valide)*
Événement 16 : Tcp_CR_Acked *(demande de connexion acquittée)*
Événement 17 : TcpConnectionConfirmed *(connexion TCP confirmée)*
Événement 18 : TcpConnectionFails *(échec de connexion TCP)*

[Événement fondés sur les messages BGP]
Événement 19 : BGPOpen *(BGP ouvert)*
Événement 20 : BGPOpen avec le temporisateur de retard d'ouverture courant
Événement 21 : BGPHeaderErr *(erreur d'en-tête BGP)*
Événement 22 : BGPOpenMsgErr *(erreur du message d'ouverture de BGP)*
Événement 23 : OpenCollisionDump *(atténuation de collisions d'ouverture)*
Événement 24 : NotifMsgVerErr *(notification d'erreur de version)*
Événement 25 : NotifMsg *(message de notification)*
Événement 26 : KeepAliveMsg *(message de garde en vie)*
Événement 27 : UpdateMsg *(message de mise à jour)*
Événement 28 : UpdateMsgErr *(erreur dans un message de mise à jour)*

3.1 Vulnérabilités des messages BGP

Il y a quatre types de messages BGP différents - OPEN *(ouverture)*, KEEPALIVE *(garder en vie)*, NOTIFICATION, et UPDATE *(mise à jour)*. Ce paragraphe contient une discussion des vulnérabilités survenant de chaque message et de la capacité des extérieurs ou homologues BGP à exploiter les vulnérabilités. Pour résumer, les extérieurs peuvent utiliser des messages OPEN, KEEPALIVE, NOTIFICATION, ou UPDATE bogués pour interrompre les connexions BGP entre les homologues BGP. Ils peuvent utiliser des messages UPDATE bogués pour interrompre l'acheminement sans casser la connexion entre les homologues. Les extérieurs peuvent aussi interrompre les connexions entre les homologues en insérant

des paquets TCP bogués qui interrompent le traitement de la connexion TCP. En général, la capacité des extérieurs à utiliser des messages BGP et TCP bogués est limitée, mais non éliminée, par le traitement du numéro de séquence TCP. L'utilisation de la [RFC2385] peut contrer ces attaques d'extérieurs. Les homologues BGP eux-mêmes ont la permission de casser des connexions d'homologue à homologue, à tout moment, en utilisant des messages NOTIFICATION. Donc, il n'y a pas de risque supplémentaire de casser les connexions par leur utilisation des messages OPEN, KEEPALIVE, ou UPDATE. Cependant, les homologues BGP peuvent interrompre l'acheminement (de façons permises) en produisant des messages UPDATE qui contiennent des informations d'acheminement boguées. En particulier, des attributs bogués ATOMIC_AGGREGATE, NEXT_HOP et AS_PATH et des NLRI dans des messages UPDATE peuvent interrompre l'acheminement. L'utilisation de la [RFC2385] ne va pas contrer ces attaques provenant d'homologues BGP.

Chaque message introduit certaines vulnérabilités et des risques, qui sont discutés dans les paragraphes suivants.

3.1.1 En-tête de message

Événement 21 : chaque message BGP commence par un en-tête standard. Dans tous les cas, des erreurs syntaxiques dans l'en-tête de message vont être cause que le locuteur BGP clôt la connexion, libère toutes les ressources BGP associées, supprime toutes les routes apprises à travers cette connexion, lance son processus de décision pour décider de nouvelles routes, et cause le retour de l'état à Repos. Aussi, facultativement, une atténuation d'oscillation spécifique de la mise en œuvre de l'homologue peut être effectuée. Le processus d'atténuation d'oscillation de l'homologue peut affecter le délai dans lequel la connexion peut être redémarrée. Un extérieur qui pourrait envoyer des messages usurpés avec des erreurs d'en-tête de message pourrait causer des interruptions dans l'acheminement à une grande échelle.

3.1.2 OPEN

Événement 19 : la réception d'un message OPEN dans les états Connecté ou Actif va causer la fermeture de la connexion par le locuteur BGP, la libération de toutes les ressources BGP associées, la suppression de toutes les routes associées, le lancement de son processus de décision, et le retour de l'état à Repos. La suppression des routes peut causer un effet de cascade dans lequel les changements d'acheminement se propagent aux autres homologues. Aussi, facultativement, une atténuation spécifique de la mise en œuvre des oscillations d'homologue peut être effectuée. Le processus d'atténuation d'oscillations de l'homologue peut affecter le délai de redémarrage de la connexion.

Dans les états OuvertConfirmé ou Établi, l'arrivée d'un OPEN peut indiquer une collision de connexions. Si cette connexion doit être abandonnée, l'événement 23 va alors être produit. (L'événement 23, discuté plus loin, résulte en le même ensemble d'actions interruptives que mentionné ci-dessus pour les états Connecté ou Actif.)

Dans l'état OuvertEnvoyé, l'arrivée d'un message OPEN va amener le locuteur BGP à passer à l'état OuvertConfirmé. Si un extérieur était capable d'usurper un message OPEN (ce qui exige une coordination temporelle très précise) l'arrivée ensuite du message OPEN de l'homologue légitime pourra conduire le locuteur BGP à déclarer une collision de connexions. La procédure de détection de collision peut causer l'abandon de la connexion légitime.

Par conséquent, la capacité d'un extérieur à usurper ce message peut conduire à une sévère interruption de l'acheminement sur une vaste zone.

Événement 20 : si un message OPEN arrive alors que le temporisateur DelayOpen court pendant que la connexion est dans l'état OuvertEnvoyé, OuvertConfirmé ou Établi, le locuteur BGP va fermer la connexion, libérer toutes les ressources BGP associées, supprimer toutes les routes associées, lancer son processus de décision, et causer le retour de l'état à Repos. La suppression des routes peut causer un effet de cascade dans lequel les changements d'acheminement se propagent aux autres homologues. Aussi, facultativement, une atténuation spécifique de la mise en œuvre des oscillations d'homologue peut être effectuée. Le processus d'atténuation d'oscillations de l'homologue peut affecter le délai de redémarrage de la connexion. Cependant, parce que le temporisateur OpenDelay ne devrait jamais fonctionner dans ces états, cet effet ne pourrait être causé que par une erreur de mise en œuvre (un message NOTIFICATION est envoyé avec le code d'erreur "Erreur d'automate à états finis"). Il serait difficile, sinon impossible, à un extérieur de produire cette erreur d'automate à états finis.

Dans les états Connecté et Actif, cet événement va causer une transition à l'état OuvertConfirmé. Comme dans l'événement 19, si un extérieur est capable de faire passer un faux OPEN, qui arrive pendant le fonctionnement du temporisateur DelayOpen, l'arrivée ultérieure de l'OPEN provenant de l'homologue légitime peut être considérée comme une collision de connexions et la connexion légitime pourrait être abandonnée.

Par conséquent, la capacité d'un extérieur à usurper ce message peut conduire à une sévère interruption de l'acheminement sur une vaste zone.

Événement 22 : Des erreurs dans le message OPEN (par exemple, un état Garde inacceptable, un paramètre facultatif mal formé, une version non prise en charge, etc.) vont causer l'abandon de la connexion par le locuteur BGP, la libération de toutes les ressources BGP associées, la suppression de toutes les routes associées, le lancement de son processus de décision, et le retour à l'état Repos. La suppression des routes peut causer un effet de cascade dans lequel les changements d'acheminement se propagent aux autres homologues. Aussi, facultativement, une atténuation spécifique de la mise en œuvre des oscillations d'homologue peut être effectuée. Le processus d'atténuation d'oscillations de l'homologue peut affecter le délai de redémarrage de la connexion. Par conséquent, la capacité d'un extérieur à usurper ce message peut conduire à une sévère interruption de l'acheminement sur une vaste zone.

3.1.3 KEEPALIVE

Événement 26 : la réception d'un message KEEPALIVE, alors que la connexion servant à la relation d'homologue à homologue est dans un des états Connecté, Actif, et OuvertEnvoyé, va causer la transition du locuteur BGP à l'état Repos et à l'échec d'établissement d'une connexion. Aussi, facultativement, une atténuation spécifique de la mise en œuvre des oscillations d'homologue peut être effectuée. Le processus d'atténuation d'oscillations de l'homologue peut affecter le délai de redémarrage de la connexion. La capacité d'un extérieur à faire passer ce message peut conduire à une interruption de l'acheminement. Pour exploiter délibérément cette vulnérabilité, le KEEPALIVE doit être inséré avec grand soin dans la séquence des messages échangés entre les homologues ; autrement, il ne causera aucun dommage.

3.1.4 NOTIFICATION

Événement 25 : la réception d'un message NOTIFICATION dans tout état va causer la suppression de la connexion par le locuteur BGP, la libération de toutes les ressources BGP associées, la suppression de toutes les routes associées, le lancement de son processus de décision, et le retour à l'état Repos. La suppression des routes peut causer un effet de cascade dans lequel les changements d'acheminement se propagent aux autres homologues. Aussi, facultativement, une atténuation spécifique de la mise en œuvre des oscillations d'homologue peut être effectuée. Le processus d'atténuation d'oscillations de l'homologue peut affecter le délai de redémarrage de la connexion. Par conséquent, la capacité d'un extérieur à usurper ce message peut conduire à une sévère interruption de l'acheminement sur une vaste zone.

Événement 24 : un message NOTIFICATION qui porte un code d'erreur de "Erreur de version" se comporte de la même façon que dans l'événement 25, avec l'exception que l'atténuation facultative d'oscillations d'homologue n'est pas effectuée dans les états OuvertEnvoyé ou OuvertConfirmé, ni dans les états Connecté ou Actif si le temporisateur DelayOpen court. Donc, le dommage causé est un peu plus petit parce que le redémarrage de la connexion n'est pas affecté.

3.1.5 UPDATE

Événement 8 : un locuteur BGP a la faculté de choisir de déconnecter automatiquement une connexion BGP si le nombre total de préfixes excède un maximum configuré. Dans ce cas, un UPDATE peut porter un nombre de préfixes qui excéderait ce maximum. Le locuteur BGP déconnecterait la connexion, libérerait toutes les ressources BGP associées, supprimerait toutes les routes associées, lancerait son processus de décision, et causerait le retour de l'état à Repos. La suppression des routes peut causer un effet de cascade dans lequel les changements d'acheminement se propagent aux autres homologues. Aussi, facultativement, une atténuation spécifique de la mise en œuvre des oscillations d'homologue peut être effectuée. Le processus d'atténuation d'oscillations de l'homologue peut affecter le délai de redémarrage de la connexion. Par conséquent, la capacité d'un extérieur à usurper ce message peut conduire à une sévère interruption de l'acheminement sur une vaste zone.

Événement 28 : si le message UPDATE est mal formé, le locuteur BGP va alors clore la connexion, libérer toutes les ressources BGP associées, supprimer toutes les routes associées, lancer son processus de décision, et causer le retour de l'état à Repos. (Ici, "mal formé" se réfère à des champs Longueur de routes retirées, Longueur totale d'attribut, ou Longueur d'attribut, impropres, à des attributs obligatoires bien connus manquants, à des fanions d'attribut qui sont en conflit avec les codes de type d'attribut, des erreurs de syntaxe dans ORIGIN, NEXT_HOP ou AS_PATH, etc.) La suppression des routes peut causer un effet de cascade dans lequel les changements d'acheminement se propagent aux autres homologues. Aussi, facultativement, une atténuation spécifique de la mise en œuvre des oscillations d'homologue peut être effectuée. Le processus d'atténuation d'oscillations de l'homologue peut affecter le délai de redémarrage de la connexion. Par conséquent, la capacité d'un extérieur à usurper ce message peut conduire à une sévère interruption de l'acheminement sur une vaste zone. Comme un locuteur BGP a l'autorité pour clore une connexion quand il veut, ce message ne donne pas aux locuteurs BGP d'opportunité supplémentaire de causer des dommages.

Événement 27 : un message UPDATE qui arrive dans tout état sauf Établi va causer la clôture de la connexion par le locuteur BGP, la libération de toutes les ressources BGP associées, la suppression de toutes les routes associées, le

lancement de son processus de décision, et le retour de l'état à Repos. La suppression des routes peut causer un effet de cascade dans lequel les changements d'acheminement se propagent aux autres homologues. Aussi, facultativement, une atténuation spécifique de la mise en œuvre des oscillations d'homologue peut être effectuée. Le processus d'atténuation d'oscillations de l'homologue peut affecter le délai de redémarrage de la connexion. Par conséquent, la capacité d'un extérieur à usurper ce message peut conduire à une sévère interruption de l'acheminement sur une vaste zone.

Dans l'état Établi, le message UPDATE porte les informations d'acheminement. La capacité de faire passer tout ou partie de ce message peut conduire à une interruption de l'acheminement, que la source du message soit un extérieur ou un locuteur BGP légitime.

3.1.5.1 Longueur des routes infaisables, Longueur totale d'attribut de chemin

Il y a une vulnérabilité qui résulte de la capacité de modifier ces champs. Si une longueur est modifiée, le message ne va probablement pas être analysé correctement, donnant une erreur, la transmission d'un message NOTIFICATION et la clôture de la connexion (voir l'événement 28, ci-dessus). Comme un vrai locuteur BGP est capable de clore une connexion à tout moment, cette vulnérabilité ne représente un risque supplémentaire que lorsque la source n'est pas l'homologue BGP configuré, c'est-à-dire qu'elle ne présente pas de risque supplémentaire de la part des locuteurs BGP.

3.1.5.2 Routes retirées

Un extérieur pourrait causer l'élimination de routes légitimes existantes en falsifiant ou en modifiant ce champ. Un extérieur pourrait aussi causer l'élimination de routes rétablies en répétant cela avec des informations de retrait provenant de paquets antérieurs.

Un locuteur BGP pourrait "faussement" retirer des routes faisables en utilisant ce champ. Cependant, comme le locuteur BGP est d'autorité pour les routes qu'il veut annoncer, il lui est permis de retirer toute route annoncée précédemment qu'il veut. Comme le locuteur BGP receveur va seulement retirer les routes associées au locuteur BGP envoyeur, il n'y a pas d'opportunité pour un locuteur BGP de retirer les routes d'un autre locuteur BGP. Donc, il n'y a pas de risque supplémentaire de la part des homologues BGP via ce champ.

3.1.5.3 Attributs de chemin

Les attributs de chemin présentent de nombreux risques et vulnérabilités différents.

o Fanions d'attribut, codes de type d'attribut, longueur d'attribut

Un homologue BGP ou un extérieur pourrait modifier la longueur d'attribut ou le type d'attribut (fanions et codes de type) pour qu'ils ne reflètent pas les valeurs d'attribut qui suivent. Si les fanions ont été modifiés, les fanions et le code de type pourraient devenir incompatibles (c'est-à-dire, un attribut obligatoire marqué comme partiel) ou un attribut facultatif pourrait être interprété comme attribut obligatoire ou vice versa. Si le code de type est modifié, la valeur de l'attribut pourrait être interprétée comme si c'était le type et la valeur de données d'un attribut différent.

Le résultat le plus probable de la modification de la longueur d'un attribut, fanion ou code de type sera une erreur d'analyse du message UPDATE. Une erreur d'analyse va causer la transmission d'un message NOTIFICATION et la fermeture de la connexion (voir l'événement 28, ci-dessus). Comme un vrai locuteur BGP est capable de clore une connexion à tout moment, cette vulnérabilité ne représente un risque supplémentaire que lorsque la source est un extérieur, c'est-à-dire, elle ne représente aucun risque supplémentaire de la part d'un homologue BGP.

o ORIGIN

Ce champ indique si les informations ont été apprises d'informations IGP ou EGP. Ce champ est utilisé pour prendre des décisions d'acheminement, de sorte qu'il y a une petite vulnérabilité d'être capable d'affecter la décision d'acheminement du locuteur BGP receveur en modifiant ce champ.

o AS_PATH

Un homologue BGP ou extérieur pourrait annoncer un AS_PATH qui n'est pas approprié pour les NLRI associées.
Comme un homologue BGP peut ne pas vérifier qu'un AS_PATH reçu commence par le numéro d'AS de son homologue, un homologue BGP malveillant pourrait annoncer un chemin qui commence par l'AS de n'importe quel locuteur BGP, avec peu d'impact sur lui-même. Cela pourrait affecter la procédure de décision du locuteur BGP receveur et son choix de la route installée. L'homologue malveillant pourrait raccourcir considérablement le AS_PATH, ce qui va augmenter les chances que cette route soit choisie, donnant éventuellement à l'homologue malveillant l'accès au trafic qu'il ne recevrait pas autrement. Le AS_PATH raccourci pourrait aussi résulter en une boucle d'acheminement, car il ne contient pas les informations nécessaires pour empêcher les boucles.

Il est possible qu'un locuteur BGP soit configuré à accepter des routes avec son propre numéro d'AS dans le chemin d'AS. De telles considérations de fonctionnement sont définies comme étant "en dehors du domaine d'application" de la spécification de BGP. Mais comme les AS_PATH peuvent légitimement faire des boucles, les mises en œuvre ne peuvent pas rejeter automatiquement les routes avec des boucles. Chaque locuteur BGP vérifie seulement que son propre numéro d'AS n'apparaît pas dans le AS_PATH.

Couplé avec la capacité d'utiliser toute valeur pour le prochain bond, cela donne à un locuteur BGP malveillant un contrôle considérable sur le chemin que le trafic va prendre.

o Routes d'origine

Un cas particulier d'annonce de faux AS_PATH se produit quand le AS_PATH annonce une connexion directe à une adresse réseau spécifique. Un homologue BGP ou extérieur pourrait interrompre l'acheminement à un ou des réseaux mentionnés dans le champ NLRI en annonçant faussement une connexion directe à ce ou ces réseaux. Les NLRI deviendraient inaccessibles à la portion du réseau qui a accepté cette fausse route, sauf si le dernier AS sur le AS_PATH entreprend de tunneler les paquets qui ont été transmis pour ces NLRI vers leur vrai AS de destination par un chemin valide. Mais même quand les paquets sont tunnelés à l'AS de destination correct, la route suivie peut n'être pas optimale, ou peut ne pas suivre la politique prévue. De plus, l'acheminement pour d'autres réseaux dans l'Internet pourrait être affecté si la fausse annonce fragmentait un bloc d'adresses agrégé, forçant les routeurs à traiter (produire des UPDATE, mémoriser, gérer) les multiples fragments plutôt que le seul agrégat. Les fausses origines d'adresses multiples peuvent résulter en l'inondation des routeurs et réseaux de transit le long de la route annoncée par du trafic en fausse direction.

o NEXT_HOP

L'attribut NEXT_HOP définit l'adresse IP du routeur frontière qui devrait être utilisé comme prochain bond lors de la transmission des NLRI mentionnées dans le message UPDATE. Si le receveur est un homologue externe, le receveur et l'adresse de prochain bond doivent alors partager un sous réseau. Il est clair qu'un extérieur qui a modifié ce champ pourrait interrompre la transmission du trafic entre les deux AS.

Si le receveur du message est un homologue externe d'un AS et si la route a été apprise d'un autre AS homologue (c'est une des deux formes de NEXT_HOP "tiers") alors le locuteur BGP qui annonce la route a l'opportunité de conduire le receveur à transmettre le trafic à un locuteur BGP à l'adresse du NEXT_HOP. Cela offre l'opportunité de diriger du trafic sur un routeur qui peut n'être pas capable de continuer la transmission du trafic. Un locuteur BGP malveillant peut aussi utiliser cette technique pour forcer un autre AS à porter du trafic qu'il n'aurait autrement pas eu à porter. Dans certains cas, ce pourrait être au bénéfice du locuteur BGP malveillant, car cela pourrait causer le transport à longue distance du trafic par l'AS victime jusqu'à un autre point d'appariement qu'il partage avec la victime.

o MULTI_EXIT_DISC

L'attribut MULTI_EXIT_DISC est utilisé dans les messages UPDATE transmis entre des homologues BGP inter AS. Bien que l'attribut MULTI_EXIT_DISC reçu d'un homologue inter AS puisse être propagé au sein d'un AS, il ne peut pas être propagé aux autres AS. Par conséquent, ce champ est seulement utilisé pour prendre des décisions d'acheminement internes à un AS. Modifier ce champ, par un extérieur ou un homologue BGP, pourrait influencer l'acheminement au sein d'un AS pour qu'il soit sous optimal, mais la portée de cet effet devrait être limitée.

o LOCAL_PREF

L'attribut LOCAL_PREF doit être inclus dans tous les messages aux homologues internes, et exclus des messages aux homologues externes. Par conséquent, la modification de LOCAL_PREF pourrait seulement affecter le processus d'acheminement au sein de l'AS. Noter qu'il n'est pas exigé par la RFC BGP que LOCAL_PREF soit cohérent entre les locuteurs BGP internes d'un AS. Comme les homologues BGP sont libres de choisir le LOCAL_PREF, la modification de ce champ est une vulnérabilité seulement à l'égard de l'extérieur.

o ATOMIC_AGGREGATE

Le champ ATOMIC_AGGREGATE indique qu'un AS quelque part le long du chemin a agrégé plusieurs routes et annoncé les NLRI agrégées sans que le AS_SET soit formé comme d'habitude à partir des AS dans les AS_PATH des routes agrégées. Les locuteurs BGP qui reçoivent une route avec ATOMIC_AGGREGATE sont empêchés de faire des NLRI plus spécifiques. Retirer l'attribut ATOMIC_AGGREGATE retirerait la restriction, causant éventuellement l'acheminement incorrect du trafic destiné aux NLRI les plus spécifiques. Ajouter l'attribut ATOMIC_AGGREGATE alors qu'aucune agrégation n'a été faite, aurait peu d'effet à part d'empêcher les NLRI non agrégées d'être rendues plus spécifiques. Cette vulnérabilité existe que la source soit un homologue BGP ou un extérieur.

o AGGREGATOR

Ce champ peut être inclus par un locuteur BGP qui a calculé les routes représentées dans le message UPDATE en agrégeant d'autres routes. Le champ contient le numéro d'AS et l'adresse IP du dernier agrégateur de la route. Il n'est pas utilisé pour prendre des décisions d'acheminement, de sorte qu'il ne représente pas une vulnérabilité.

3.1.5.4 NLRI

En modifiant ou falsifiant ce champ, une source extérieure ou homologue BGP pourrait causer l'interruption de l'acheminement au réseau annoncé, surcharger un routeur le long de la route annoncée, causer la perte de données quand la route annoncée ne va pas transmettre de trafic au réseau annoncé, acheminer le trafic par une route sous optimale, etc.

3.2 Vulnérabilités à travers d'autres protocoles

3.2.1 Messages TCP

BGP fonctionne sur TCP. Donc, BGP est l'objet d'attaques à travers les attaques sur TCP.

3.2.1.1 SYN TCP

Inondation de SYN : comme les autres protocoles, BGP est soumis aux effets des attaques d'inondation de SYN sur une mise en œuvre de TCP, et doit s'appuyer sur les protections de la mise en œuvre contre ces attaques.

Événement 14 : si un extérieur est capable d'envoyer un SYN au locuteur BGP au moment approprié durant l'établissement de la connexion, le SYN de l'homologue légitime va apparaître comme étant d'une seconde connexion. Si l'extérieur était capable de continuer avec une séquence de paquets résultant en une connexion BGP (en devinant le choix du locuteur BGP du numéro de séquence sur le SYN ACK, par exemple) la connexion de l'extérieur et la connexion de l'homologue légitime vont apparaître comme une collision de connexions. Selon le résultat de la détection de collision (c'est-à-dire, si l'extérieur choisit un identifiant BGP qui lui permet de gagner la course) la vraie connexion de l'homologue légitime pourrait être supprimée. L'utilisation de TCP MD5 peut contrer cette attaque.

3.2.1.2 SYN ACK TCP

Événement 16 : si un extérieur est capable de répondre au SYN TCP d'un locuteur BGP avant l'homologue légitime, le SYN-ACK de l'homologue légitime va recevoir une réponse ACK vide, causant la production par l'homologue légitime d'un RST qui va couper la connexion. Le locuteur BGP va terminer la connexion, libérer toutes les ressources BGP associées, supprimer toutes les routes associées, et lancer son processus de décision. Cette attaque exige que l'extérieur soit capable de prédire le numéro de séquence utilisé dans le SYN. L'utilisation de TCP MD5 peut contrer cette attaque.

3.2.1.3 ACK TCP

Événement 17 : si un extérieur était capable d'usurper un ACK au moment approprié durant l'établissement de la connexion, le locuteur BGP considérerait alors que la connexion est réalisée, enverrait un OPEN (événement 17) et passerait à l'état OuvertEnvoyé. À l'arrivée de l'ACK de l'homologue légitime, celui-ci ne va pas être livré au processus BGP, car il va être considéré comme un paquet dupliqué. Donc, ce message ne représente pas une vulnérabilité pour BGP durant l'établissement de la connexion. Usurper un ACK après l'établissement de la connexion exige la connaissance des numéros de séquence utilisés, et c'est, en général, une tâche très difficile. L'utilisation de TCP MD5 peut contrer cette attaque.

3.2.1.4 RST/FIN/FIN-ACK TCP

Événement 18 : si un extérieur est capable d'usurper un RST, le locuteur BGP va terminer la connexion, libérer toutes les ressources BGP associées, supprimer toutes les routes associées, et lancer son processus de décision. Si un extérieur est capable d'usurper un FIN, les données pourraient alors encore être transmises, mais toute tentative de les recevoir déclencherait une notification que la connexion est en cours de fermeture. Dans la plupart des cas, il en résulte que la connexion est placée dans l'état Repos. Mais si la connexion est dans l'état Connecté ou OuvertEnvoyé à ce moment, la connexion va retourner à l'état Actif.

Usurper un RST dans cette situation exige d'un extérieur qu'il devine un numéro de séquence qui doit seulement être dans la fenêtre de réception [Watson04]. C'est généralement une tâche plus facile que de deviner le numéro de séquence exact requis pour usurper un FIN. L'utilisation de TCP MD5 peut contrer cette attaque.

3.2.1.5 DoS et DDos

Comme les paquets dirigés sur l'accès TCP 179 sont passés au processus BGP, qui réside potentiellement sur un processeur plus lent dans le routeur, inonder un routeur avec des paquets à l'accès TCP 179 est un boulevard pour les attaques de DoS contre le routeur. Aucun mécanisme BGP ne peut déjouer de telles attaques ; d'autres mécanismes doivent être employés.

3.2.2 Autres protocoles de soutien

3.2.2.1 Arrêt manuel

Événement 2 : un événement d'arrêt manuel cause la fermeture de la connexion par le locuteur BGP, la libération de toutes les ressources BGP associées, la suppression de toutes les routes associées, et le lancement de son processus de décision. Si le mécanisme par lequel un locuteur BGP a été informé d'un arrêt manuel n'est pas protégé avec soin, la connexion BGP pourrait être détruite par un extérieur. Par conséquent, la sécurité de BGP dépend en second de la sécurité des protocoles de gestion et de configuration qui sont utilisés pour signaler cet événement.

3.2.2.2 Atténuation de collision ouverte

Événement 23 : l'événement OpenCollisionDump *(vidage de collision d'ouverture)* peut être généré administrativement quand un événement de collision de connexions est détecté et que la connexion a été choisie comme étant celle qui doit être déconnectée. Quand cet événement se produit dans tout état, la connexion BGP est abandonnée, les ressources BGP sont libérées, les routes associées sont supprimées, etc. Par conséquent, la sécurité de BGP dépend en second de la sécurité des protocoles de gestion et de configuration utilisés pour signaler cet événement.

3.2.2.3 Événements de temporisateur

Événements 9-13 : BGP emploie cinq temporisateurs (ConnectRetry, Hold, Keepalive, MinASOrigination-Interval, et MinRouteAdvertisementInterval) et deux temporisateurs facultatifs (DelayOpen et IdleHold). Ces temporisateurs sont critiques pour le fonctionnement de BGP. Par exemple, si la valeur du temporisateur de garde était changée, l'homologue distant pourrait considérer que la connexion ne répond pas et la fermer, libérant ainsi les ressources, supprimant les routes associées, etc. Par conséquent, la sécurité de BGP dépend en second de la sécurité des protocoles de fonctionnement, gestion et configuration qui sont utilisés pour modifier les temporisateurs.

4. Considérations sur la sécurité

Ce mémoire tout entier concerne la sécurité, et il décrit et analyse les vulnérabilités qui existent dans BGP.

L'utilisation des mécanismes de prise en charge obligatoire de la [RFC2385] contre les attaques d'insertion, suppression, et modification de messages, ainsi que les attaques par interposition par des extérieurs. Si la confidentialité des données d'acheminement est désirée (il y a une controverse sur le point de savoir si c'est un service de sécurité souhaitable) l'utilisation de IPsec ESP pourrait fournir ce service.

4.1 Risque résiduel

Comme mécanismes fondés sur le chiffrement, TCP MD5 [RFC2385] et IPsec [RFC2401] supposent que les algorithmes cryptographiques sont sûrs, que les secrets utilisés sont protégés contre l'exposition et sont bien choisis de façon à n'être pas faciles à deviner, que les plates-formes sont gérées de façon sûre et fonctionnent sans permettre les intrusions, etc.

Ces mécanismes n'empêchent pas les attaques qui proviennent des homologues légitimes d'un routeur. Il y a plusieurs solutions possibles pour empêcher un locuteur BGP d'insérer des informations boguées dans ses annonces à ses homologues (c'est-à-dire, de monter une attaque sur l'origine ou l'AS-PATH d'un réseau) :
(1) protection de l'origine : signer l'AS d'origine ;
(2) protection de l'origine et des adjacences : signer les informations de l'AS d'origine et du prédécesseur [Smith96] ;
(3) protection de l'origine et de la route : signer l'AS d'origine, et incorporer les signatures des AS_PATH au numéro des mauvais routeurs consécutifs dont on veut éviter qu'ils causent des dommages [SBGP00] ;
(4) filtrage : s'appuyer sur un registre pour vérifier l'AS qui génère le AS_PATH et les NLRI [RFC2725].

Le filtrage est en usage sur certains points de rattachement de consommateurs, mais n'est pas effectif près du centre de l'Internet. Les autres mécanismes font l'objet de controverses et ne sont pas encore d'usage courant.

4.2 Protections du fonctionnement

BGP est principalement utilisé comme moyen de fournir des informations d'accessibilité au système autonome (AS) et de distribuer en interne l'accessibilité externe au sein d'un AS. BGP est le protocole d'acheminement utilisé pour distribuer les

informations d'acheminement global dans l'Internet. Donc, BGP est utilisé par tous les fournisseurs d'accès Internet (FAI) majeurs, ainsi que par de nombreux petits fournisseurs et autres organisations.

Les rôle de BGP dans l'Internet met les mises en œuvre de BGP dans des conditions uniques, et fait peser des exigences de sécurité uniques sur BGP. BGP fonctionne sur des interfaces inter fournisseurs dans lesquelles les niveaux de trafic poussent l'état de l'art dans le matériel de transmission de paquet spécialisé et excèdent les capacités de performance de la mise en œuvre de matériel de déchiffrement de nombreux ordres de grandeur. La capacité d'un attaquant utilisant une seule station de travail avec une interface haut débit pour générer du faux trafic pour du déni de service excède de loin la capacité de déchiffrement fondé sur le logiciel ou de matériel cryptographique de prix approprié pour détecter le faux trafic. Dans ces conditions, un moyen pour protéger les éléments de réseau des attaques de DoS est d'utiliser des techniques de filtrage fondées sur le paquet sur la base d'une relativement simple inspection des paquets. Par suite, pour un FAI qui porte de gros volumes de trafic, la capacité de filtrer les paquets sur la base des numéros d'accès est une importante protection contre les attaques de DoS, et un ajout nécessaire à la force cryptographique dans l'encapsulation.

La pratique courante des FAI est d'utiliser certaines techniques de filtrage communes pour réduire l'exposition aux attaques provenant de l'extérieur du FAI. Pour protéger les sessions de BGP internes (IBGP) les filtres sont appliqués à toutes les frontières du réseau d'un FAI. Cela supprime tout le trafic destiné aux adresses internes des éléments de réseau (normalement contenues dans un seul préfixe) et au numéro d'accès BGP (179). Si le numéro d'accès BGP est trouvé, les paquets provenant de l'intérieur du FAI ne sont pas transmis à partir d'une interface interne à l'adresse du locuteur BGP (sur laquelle les sessions BGP externes (EBGP) sont prises en charge) ou d'une adresse EBGP d'un homologue. Une conception approprié de routeur peut limiter le risque de compromission quand un homologue BGP échoue à fournir un filtrage adéquat. Le risque peut être limité à la session d'homologue à homologue sur laquelle le filtrage n'est pas effectué par l'homologue, ou à l'interface ou carte de ligne sur laquelle l'appariement est pris en charge. Il y a des motifs substanciels, et peu d'efforts sont nécessaires, pour que les FAI utilisent de tels filtres.

Ces pratiques de fonctionnement élèvent considérablement la difficulté pour un extérieur de lancer une attaque de déni de service contre un FAI. En empêchant d'injecter le trafic suffisant à partir de l'extérieur d'un réseau pour effectuer une attaque de déni de service, l'attaquant devrait entreprendre des tâches plus difficiles, comme de compromettre des éléments de réseau du FAI ou une surveillance non détectée dans des supports physiques.

5. Références

5.1 Références normatives

[RFC2119] S. Bradner, "Mots clés à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, mars 1997. *(MàJ par* RFC8174)

[RFC2385] A. Heffernan, "Protection des sessions de BGP via l'option de signature MD5 de TCP", août 1998. *(P.S. ; MàJ par la* RFC6691*) ; remplacée par* RFC5925)

[RFC4271] Y. Rekhter, T. Li et S. Hares, "Protocole de routeur frontière version 4 (BGP-4)", janvier 2006. *(D.S.) (MàJ par* RFC6608, RFC8212)

5.2 Références pour information

[RFC2401] S. Kent et R. Atkinson, "Architecture de sécurité pour le protocole Internet", novembre 1998. (*Obsolète, voir* RFC4301)

[RFC2725] C. Villamizar et autres, "Sécurité du système de politique d'acheminement", décembre 1999. (*MàJ par* RFC4012) *(P.S.)*

[RFC3552] E. Rescorla, B. Korver, "Lignes directrices pour la rédaction d'une section de considérations sur la sécurité dans les RFC", juillet 2003. (BCP0072)

[SBGP00] Kent, S., Lynn, C. et Seo, K., "Secure Border Gateway Protocol (Secure-BGP)", IEEE Journal on Selected Areas in Communications, Vol. 18, n° 4, avril 2000, pp. 582-592.

[Smith96] Smith, B. et Garcia-Luna-Aceves, J.J., "Securing the Border Gateway Routing Protocol", Proc. Global Internet '96, London, UK, 20-21 novembre 1996.

[Watson04] Watson, P., "Slipping In The Window: TCP Reset Attacks", CanSecWest 2004, avril 2004.

Adresse de l'auteur

Sandra Murphy
Sparta, Inc.
7075 Samuel Morse Drive
Columbia, MD 21046
USA
mél : Sandy@tislabs.com

Déclaration complète de droits de reproduction

Remerciement
Le financement de la fonction d'édition des RFC est actuellement fourni par la Internet Society.