Network Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: May 7, 2020

H. Chen
China Telecom
D. Ma
ZDNS
Y. Gu
S. Zhuang
H. Wang
Huawei

November 4, 2019

Enhanced AS Loop Detection for BGP
draft-chen-grow-enhanced-as-loop-detection-03

Abstract

Misconfiguration and malicious manipulation of BGP AS_Path may lead to route hijack. This document proposes to enhance the BGP Inbound/Outbound route processing in the case of detecting an AS loop. Two options are proposed for the enhancement, a) a local check at the device; b) data collection/analysis at the remote network controller/server. Both approaches are beneficial for route hijack detection.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The Border Gateway Protocol (BGP) [RFC4271], as an inter-Autonomous (AS) routing protocol, is used to exchange network reachability information between BGP systems. As a distance-vector based protocol, special mechanism is designed for BGP to avoid routing loop. As stated in Section 9.1.2. of RFC4271:

> ...
>
> If the AS_PATH attribute of a BGP route contains an AS loop, the BGP route should be excluded from the Phase 2 decision function. AS loop detection is done by scanning the full AS path (as specified in the AS_PATH attribute), and checking that the autonomous system number of the local system does not appear in the AS path. Operations of a BGP speaker that is configured to

accept routes with its own autonomous system number in the AS path are outside the scope of this document.

...

Conventionally, upon receiving an BGP Update route with as loop detection, the route is simply discarded. In the case of forged-AS-type BGP hijacks, which can be generated by configuration errors or malicious attacks, the simple discard action can lead to large-scale network connectivity issues.

This document proposes enhancements to BGP inbound and outbound processing when detecting AS loop in order to identify possible BGP hijacks.

2. Terminology

The following terminology is used in this document.

AS: Autonomous System

BGP: Border Gateway Protocol

ROA: Route Origin Authorization

ASPA: Autonomous System Provider Authorization

ISP: Internet Service Provider

BMP: BGP Monitoring Protocol

3. Forged AS_PATH Examples

3.1. AS Loop Detected at Inbound Processing

- Forged Case 1: AS shown in Figure 1, an upstream AS of AS64596 forged a route with the ASN 64596 as the origin ASN in the AS-Path.

- Forged Case 2: AS shown in Figure 1, an upstream AS of AS64596 forged a route with the ASN 64596 as the transit ASN in the AS-Path.

```
            AS Loop Detection enhancement point
                             |
                             |                     x.y.z.0/24
                             |                Origin AS 64600
                             v               <----------------
   AS64595---AS64596---AS64597---AS64598---AS64599----AS64600
                       Normal Case:
                       x.y.z.0/24, AS-Path: 64598 64599 64600

                       Forged Case 1:
                       x.y.z.0/24, AS-Path: 64598 64597

                       Forged Case 2:
                       x.y.z.0/24, AS-Path: 64598 64597 64600
```

Figure 1: BGP Inbound Route Processing

3.2. AS Loop Detected at Outbound Processing

- o Forged Case 3: AS shown in Figure 2, an upstream AS of AS64597 forged a route with the ASN 64596 as the origin ASN in the AS-Path.

- o Forged Case 4: AS shown in Figure 2, an upstream AS of AS64597 forged a route with the ASN 64596 as the transit ASN in the AS-Path.

```
         AS Loop Detection enhancement point
                       |
                       |                         x.y.z.0/24
                       |                     Origin AS 64600
                       v                   <----------------
   AS64595---AS64596---AS64597---AS64598---AS64599----AS64600
                       Normal Case:
                       <-- x.y.z.0/24, AS-Path: 64597 64598 64599 64600

                       Forged Case 3:
                       <-- x.y.z.0/24, AS-Path: 64597 64598 64596

                       Forged Case 4:
                       <-- x.y.z.0/24, AS-Path: 64597 64596 64600
```

Figure 2: BGP Outbound Route Processing

4. Enhancement to BGP Inbound/Outbound Processing

4.1. Enhancement for AS Loop Detected at Inbound Process

Currently, ROV [RFC6811] and ASPA verification [I-D.ietf-sidrops-aspa-verification]can be adopted for BGP leak/ hijack detection. However, for the forged case 1&2, the conventional BGP inbound process would simply discard the routes with AS loop before any further leak/hajack detection.

This document suggests further analysis of such routes. The analysis may include mechanisms that apply to normal routes for hijack detection, such as ROV, ASPA and so on. The detailed analyzing mechanisms as well as the corresponding actions w.r.t. the analysis are outside the scope of this document.

Two options of where the analysis of the inbound processing enhancement takes place is proposed.

- Option 1: Analyze the routes with AS loop based on local database.

- Option 2: Collect the routes with AS loop with BMP and analyze them at the remote controller/server.

4.2. Enhancement for AS Loop Detected at Outbound Process

Currently, the egress ROV can be adopted for BGP hijack detection. However, for forged case 3&4, when eBGP Split-Horizon is enabled, the routes with AS loop could possibly be discarded before any hijack detection.

This document suggests further analysis of such routes. The analysis may include mechanisms that apply to normal routes for hijack detection, such as egress ROV, ASPA and so on. The detailed analyzing mechanisms as well as the corresponding actions w.r.t. the analysis are outside the scope of this document.

Two options of where the analysis of the outbound processing enhancement takes place is proposed.

- Option 1: Analyze the routes with AS loop based on local database.

- Option 2: Collect the routes with AS loop with BMP and analyze them at the remote controller/server.

5. BMP extension for AS Loop Detection

This document extends the BMP Route Mirroring message to mirror routes with AS loop to the BMP Server.

Per RFC7854, Route Mirroring messages can be used to mirror the messages that have been treated-as-withdraw [RFC7606], for debugging purposes. This document defines a new code type for Type 1 Information TLV:

- o Code = TBD: AS Loop Detected. An AS loop is detected for the BGP route. A BGP Message TLV MUST also occur in the TLV list.

6. Acknowledgements

The authors would like to acknowledge the review and inputs from Gang Yan, Zhenbin Li, Aijun Wang, Jeff Haas, Robert Raszuk, Chris Morrow, Alexander Asimov, Ruediger Volk, Jescia Chen and the working group.

7. IANA Considerations

This document defines one type for information carried in the Route Mirroring Information (Section 4.7 of RFC7854) code:

- o Code = TBD: AS Path Looped.

8. Security Considerations

This document does not change the underlying security issues in the BGP protocol. It however, does provide an additional mechanism to protect against attacks based on the forged AS-Path in the BGP routes.

9. Normative References

[I-D.ietf-sidrops-aspa-verification]
Azimov, A., Bogomazov, E., Patel, K., and J. Snijders, "Verification of AS_PATH Using the Resource Certificate Public Key Infrastructure and Autonomous System Provider Authorization", draft-ietf-sidrops-aspa-verification-01 (work in progress), July 2019.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4271] Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, DOI 10.17487/RFC4271, January 2006, <https://www.rfc-editor.org/info/rfc4271>.

[RFC4760] Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, DOI 10.17487/RFC4760, January 2007, <https://www.rfc-editor.org/info/rfc4760>.

[RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, DOI 10.17487/RFC6811, January 2013, <https://www.rfc-editor.org/info/rfc6811>.

[RFC7854] Scudder, J., Ed., Fernando, R., and S. Stuart, "BGP Monitoring Protocol (BMP)", RFC 7854, DOI 10.17487/RFC7854, June 2016, <https://www.rfc-editor.org/info/rfc7854>.

Authors' Addresses

Huanan Chen
China Telecom
109, West Zhongshan Road, Tianhe District
Guangzhou 510000
China

Email: chenhn8.gd@chinatelecom.cn

Di Ma
ZDNS
4 South 4th St. Zhongguancun
Beijing, Haidian
China

Email: madi@zdns.cn

Yunan Gu
Huawei
Huawei Bld., No.156 Beiqing Rd.
Beijing 100095
China

Email: guyunan@huawei.com

Shunwan Zhuang
Huawei
Huawei Bld., No.156 Beiqing Rd.
Beijing 100095
China

Email: zhuangshunwan@huawei.com

Haibo Wang
Huawei
Huawei Bld., No.156 Beiqing Rd.
Beijing 100095
China

Email: rainsword.wang@huawei.com