SIDROPS
Internet-Draft
Intended status: Informational
Expires: 8 June 2026

S. Wang
Beijing Zhongguancun Laboratory
K. Xu
Q. Li
Z. Liu
Beijing Zhongguancun Laboratory and Tsinghua University

5 December 2025

Issue in Route Origin Validation from Route Partial Visibility
draft-wang-sidrops-route-partial-visibility-01

Abstract

In the Resource Public Key Infrastructure (RPKI), validating prefix-origin pairs using Route Origin Authorizations (ROAs) globally and performing Route Origin Validation (ROV) locally at each Autonomous System (AS) with validated ROA payloads (VRPs) can lead to inconsistent results due to partial route visibility. This document highlights how partial route visibility can turn originally non-loose ROAs into loose VRPs, outlines the causes of partial route visibility, and discusses potential solutions to mitigate the issue.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 8 June 2026.

Table of Contents

1. Introduction

Route hijacking is a significant vulnerability in the Border Gateway Protocol (BGP) due to lack of restrictions on prefix ownership claims. To combat this, the Resource Public Key Infrastructure (RPKI) [RFC6482] was introduced to validate prefix-origin pairs. Prefix owners issue Route Origin Authorizations (ROAs) specifying the prefix-origin pairs to RPKI repositories. Relying parties (RPs) in each autonomous system (AS) then download the ROAs, generate Validated ROA Payloads (VRPs), and distribute them to border routers. These routers use VRPs to perform Route Origin Validation (ROV) [RFC6483][RFC6811].

A common misconception is that without engineering errors (e.g., issues with the RPKI repository, RP malfunctions, or ROV execution failures), a secure ROA would yield a secure VRP in certain. "Secure" means each covered prefix is protected from route hijacking. However, in reality, routes from the origin AS and the corresponding ROAs travel through different channels. Routes are distributed via

BGP and may be affected by transit AS policies. In contrast, ROAs are stored in global RPKI repositories, so they are accessible to RPs in all locations. This divergence can lead to inconsistencies between validation using ROAs from global repositories and ROV with local VRPs.

This memo will first address the problem of route partial visibility: validation of routes could be inconsistent with either ROAs or VRPs. Then possible causes which could lead to route partial visibility are summarized. Finally, the memo will discuss potential solutions to resolve or mitigate the resulting vulnerabilities.

2. 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 [RFC2119].

3. Problem Statement

The concept of a "loose" ROA is defined as, a ROA whose sub-prefixes of the maximum length allowed by itself are not always advertised in BGP [RFC9319]. For example, in Figure 1, within the prefix range 185.70.140.0/22-24, AS 201411 originates two prefixes, B (185.70.140.0/23) and D (185.70.140.0/24), and issues a ROA (AS 201411, 185.70.140.0/23-24), marked with asterisks (*). Any other prefixes in this prefix range are not announced by any AS. Since prefix E (185.70.141.0/24) is not announced, the ROA is considered loose.

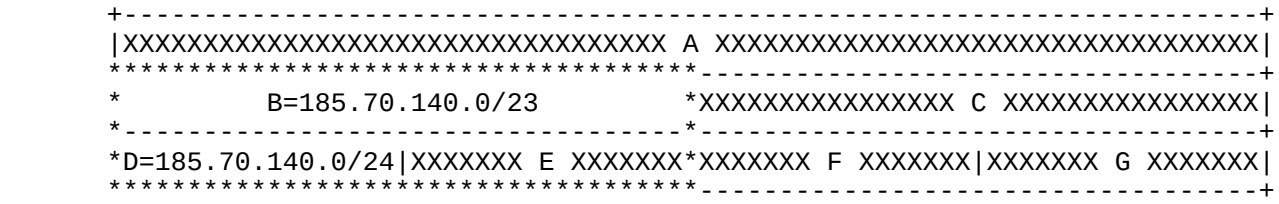

Figure 1: an example of loose ROA

3.1. Vulnerabilities of Loose ROAs

A sub-prefix S which causes a ROA to be loose faces two primary vulnerabilities:

* Super-prefix Hijacking: An attacker can announce a super-prefix of S, such as A (185.70.140.0/22) in Figure 1, with the same origin AS. This route will be validated as "not-found" since its prefix length is shorter than the ROA's prefix range (23-24) and won't be filtered. Because prefix E (185.70.141.0/24) is not announced, the attack route will be the best route for addresses in prefix E, leading to traffic hijacking.

* Forged-Origin Hijacking: An attacker can announce a route with S and the original AS as the origin but with a fake AS path that includes the attacker' s AS. This type of hijacking can also affect non-loose ROAs but is guaranteed to succeed against loose ROAs. In Figure 1, if an attacker announces prefix E with an AS path ending in AS 201411, it will be validated as "valid" and selected as the best route for addresses in prefix E. Consequently, traffic will follow the attack route into the attacker's AS, resulting in hijacking.

3.2. Refined Definitions for Loose ROAs and VRPs

The previous definition of loose ROAs misses certain corner cases. For example, in Figure 2, AS 201411 originates two prefixes, D (185.70.140.0/24) and E (185.70.141.0/24), but issues three ROAs: (AS 201411, 185.70.140.0/23-23), (AS 201411, 185.70.140.0/24-24), and (AS 201411, 185.70.141.0/24-24). These can be combined into one single ROA (AS 201411, 185.70.140.0/23-24). This ROA is not loose because all its sub-prefixes of the maximum length allowed are advertised in BGP.

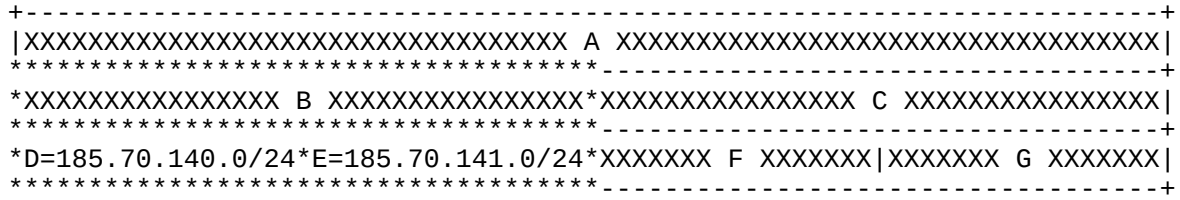

Figure 2: an example of non-loose ROA

Therefore, for a strict definition, a ROA is non-loose if, for any address I covered by the ROA R, there exists an advertised route that:

1. Covers I.

2. Is validated as valid (not necessarily by R).

3. Has the longest prefix length among advertised routes whose prefixes cover I.

4. Has a prefix length greater than or equal to R' s MaxLength (Lm).

If these conditions are not met, the ROA R is considered loose.

Since VRPs are derived from ROAs, "loose VRPs" can be similarly defined from "loose ROAs." The main difference is that for VRPs, "the route should be advertised" changes to "the route should be in the router' s local RIB" (Routing Information Base). This is because ROAs apply to globally announced routes, while VRPs are used within each AS and validate locally received routes. Therefore, only routes visible to the local router determine VRP looseness.

Therfore, a VRP is non-loose if, for any address I covered by the VRP V on a border router, there always exists a route in the router's local RIB that:

1. Covers I.

2. Is validated as valid (not necessarily by V).

3. Has the longest prefix length among all routes in the local RIB whose prefixes cover I.

4. Has a prefix length greater than or equal to V' s MaxLength (Lm).

If these conditions are not met, the VRP V is considered loose.

3.3. Route Partial Visibility

In theory, the origin AS can control its own ROA issuance to ensure consistency with its advertised routes but cannot ensure other ASes will receive these routes precisely. A route initially announced may fail to propagate to another AS. If this route's prefix is a sub-prefix within the maximum length allowed by the origin AS's ROA, the resulting VRP at the observer AS will be loose. We term this phenomenon, where a route announced with a ROA is not visible to all ASes, as route partial visibility.

In conclusion, a key issue with ROV is that non-loose ROAs don't always produce non-loose VRPs due to the partial visibility of announced routes.

4. Causes of Route Partial Visibility

The general process for the formation of route partial visibility is outlined as follows. For a given origin AS, it issues ROAs for all its active and advertised prefixes, ensuring these ROAs are initially non-loose. "Active" means that neither the prefixes nor their sub-prefixes are expired or revoked. However, when a route from the origin AS reaches a transit AS, certain BGP routing policies may alter it. This could involve dropping the route, or changing its prefix or origin AS and then propagating the modified route.

If the route is dropped, any AS that does not receive it will likely have loose VRPs. Even if the route is altered but not dropped, the VRP at an observer AS may still become loose, since the prefix may no longer match with the VRP. These transit AS policies, which we term "policies with hidden danger," inadvertently disrupt RPKI ROV. Below are possible types of policies that may drop or alter passing routes.

4.1. Explicit Route Filtering

The simplest type of policy is explicit route filtering, including import/export filtering, route blackholing, route damping, and similar mechanisms. When a transit AS applies such policies, it directly drops routes for specific prefixes. As a result, these prefixes will have no corresponding routes in the downstream ASes of the transit AS.

4.2. Implicit Route Filtering

When certain policies combine, they can implicitly drop routes. Consider this scenario in Figure 3: a MOAS prefix is announced by different ASes (AS a and AS b), with only AS a issuing a ROA for the prefix. Both routes reach an ROV-disabled AS (AS d), where the route selection policy retains only one route per prefix. Due to a shorter AS path, AS d keeps the route from AS b and discards the valid route from AS a.

This route from AS b continues spreading until it reaches an ROV-enabled AS (AS e). Since the prefix has a ROA only for AS a, the ROV policy at AS e marks the route from AS b as invalid and drops it. Consequently, there will be no route for the MOAS prefix in downstream ASes.

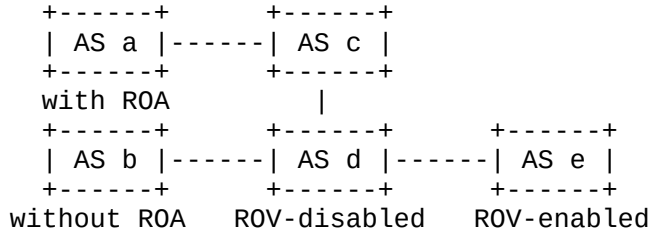

Figure 3: an example scenario of implicit route filtering

4.3. Route De-aggregation

In addition to dropping routes, routing policies can also transform prefixes within routes. One such transformation is route de-aggregation. In this process, the origin AS remains unchanged, but the original route is replaced with one or more routes for the sub-prefixes. If any de-aggregated prefix exceeds the maxLength specified in its matching VRP, it will be validated as invalid and get dropped, making the de-aggregation ineffective. Additionally, the absence of routes for the de-aggregated prefixes can make the VRP loose.

4.4. Route Aggregation

The opposite transformation is route aggregation. Route aggregation suppresses the original routes and generates a new route with a super-prefix encompassing all original prefixes. The ROV status of the aggregated route can vary:

1. Valid: If the aggregated prefix has a ROA and the origin AS matches the transit AS performing the aggregation.

2. Not Found: If no ROA exists for the aggregated prefix. For a successful super-prefix hijack, the attack route must be shorter than all original prefixes but not shorter than the aggregated prefix.

3. Invalid: If another ROA exists for a different origin AS for the aggregated prefix or any super-prefix of it, causing the aggregated route to be filtered and the aggregation to fail. Additionally, the absence of routes for the de-aggregated prefix may contribute to VRP looseness.

5. Potential Solutions

Since there is no prior work formally addressing the problem, no solutions exist to systematically eliminate the issue in ROV with route partially visibility. Generally, there are two main approaches to address the problem: one is to eliminate potential risks by addressing policies with hidden dangers, and the other is to defend against damages when attacks occur due to these policies.

5.1. Report Policies with Hidden Danger

To resolve the issue fundamentally, transit ASes must report policies with potential hidden dangers. The reporting approach depends on the policy type:

* Route Filtering: ROAs cannot prevent super-prefix hijacks since an attacker can always announce a route with a shorter prefix, making its ROV state "not found." Ideally, the transit AS should inform all its downstream ASes about the filtered routes, allowing them to inspect overlapping prefixes in their received routes.

* Route Transformation (Aggregation or De-aggregation): The transit AS should notify the origin ASes. For de-aggregation, origin ASes should issue additional ROAs for the de-aggregated prefixes. For aggregation, the transit AS should additionally obtain permissions from all origin ASes to announce a ROA itself for the aggregated prefix.

Implementing this proposal is challenging for several reasons. First, transit ASes may be reluctant to disclose routing policies for security reasons and see no benefit, as their own policies do not affect them negatively. Second, malicious transit ASes might provide false information about their policies. Additionally, other ASes may be unwilling to adjust their routing policies or ROAs based on claims from another AS.

5.2. Defend Against Attacks Exploiting Loose VRPs

A more practical approach is to let each observer AS handle the defense, without involving the transit AS. While observer ASes may not know which routes are partially visible to them, they can still defend against potential forged-origin and super-prefix hijacks.

There are already many recent studies focusing on defending forged-origin hijacks, and their main idea is combining the AS path feature and validating the AS path of received routes, such as using ASPA [I-D.ietf-sidrops-aspa-verification].

For super-prefix hijacks, solutions fall into two categories:

* At RPKI Level: Observer ASes can independently add, delete, or modify local VRPs using techniques such as SLURM [RFC8416], which is effective for route transformations.

* At BGP Level: Observer ASes can add blocking rules or make blackhole announcements for routes that could trigger super-prefix hijacks, which is suitable for route filtering.

In summary, defending against the vulnerabilities of loose VRPs requires systematic efforts.

6. Security Considerations

There is no security consideration in this draft.

7. IANA Considerations

There is no IANA consideration in this draft.

8. References

8.1. Normative References

[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>.

[RFC6482] Lepinski, M., Kent, S., and D. Kong, "A Profile for Route Origin Authorizations (ROAs)", RFC 6482, DOI 10.17487/RFC6482, February 2012, <https://www.rfc-editor.org/info/rfc6482>.

[RFC6483] Huston, G. and G. Michaelson, "Validation of Route Origination Using the Resource Certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs)", RFC 6483, DOI 10.17487/RFC6483, February 2012, <https://www.rfc-editor.org/info/rfc6483>.

[RFC6811] Mohapatra, P., Scudder, J., Ward, D., Bush, R., and R. Austein, "BGP Prefix Origin Validation", RFC 6811, DOI 10.17487/RFC6811, January 2012, <https://www.rfc-editor.org/info/rfc6811>.

8.2. Informative References

[RFC8416] Ma, D., Mandelberg, D., and T. Bruijnzeels, "Simplified Local Internet Number Resource Management with the RPKI (SLURM)", RFC 8416, DOI 10.17487/RFC8416, August 2018, <https://www.rfc-editor.org/info/rfc8416>.

[RFC9319] Gilad, Y., Goldberg, S., Sriram, K., Snijders, J., and B. Maddison, "The Use of maxLength in the Resource Public Key Infrastructure (RPKI)", RFC 9319, DOI 10.17487/RFC9319, January 2012, <https://www.rfc-editor.org/info/rfc9319>.

[I-D.ietf-sidrops-aspa-verification] Azimov, A., Bogomazov, E., Bush, R., Patel, K., Snijders, J., and K. Sriram, "BGP AS_PATH Verification Based on Autonomous System Provider Authorization (ASPA) Objects", Work in Progress, Internet-Draft, draft-ietf-sidrops-aspa-verification-19, 27 September 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-sidrops-aspa-verification-19>.

Authors' Addresses

Shuhe Wang
Beijing Zhongguancun Laboratory
Building 8, CourtYard 1, Zhongguancun East Road, Haidian District
Beijing
China
Email: wangsh@mail.zgclab.edu.cn

Ke Xu
Beijing Zhongguancun Laboratory and Tsinghua University
Beijing
China
Email: xuke@zgclab.edu.cn

Qi Li
Beijing Zhongguancun Laboratory and Tsinghua University
Beijing
China
Email: liqi@zgclab.edu.cn

Zhuotao Liu
Beijing Zhongguancun Laboratory and Tsinghua University
Beijing
China
Email: liuzhuotao@zgclab.edu.cn