SIDR Operations
Internet-Draft
Intended status: Informational
Expires: 10 February 2023

Z. Yan
CNNIC
R. Bush
Internet Initiative Japan
G.G. Geng
Jinan University
T. de Kock
RIPE NCC

August 2022

Avoidance for ROA Containing Multiple IP Prefixes
draft-ietf-sidrops-roa-considerations-03

Abstract

In RPKI, the address space holder needs to issue an ROA object when authorizing one or more ASes to originate routes to IP prefix(es). During ROA issurance process, the address space holder may need to specify an origin AS for a list of IP prefixes. Additionally, the address space holder is free to choose to put multiple prefixes into a single ROA or issue separate ROAs for each prefix according to the current specification. This memo analyzes some operational problems which may arise from ROAs containing multiple IP prefixes and recommends avoiding placing multiple IP prefixes in one ROA.

Table of Contents

1. Introduction

In Resource Public Key Infrastructure (RPKI), Route Origin Authorization (ROA) is a digitally signed object which identifies that a single AS has been authorized by the address space holder to originate routes to one or more prefixes within the address space[RFC6482].

Each ROA contains an "asID" field and an "ipAddrBlocks" field. The "asID" field contains one single AS number which is authorized to originate routes to the given IP address prefixes. The "ipAddrBlocks" field contains one or more IP address prefixes to which the AS is authorized to originate the routes. If the address space holder needs to authorize more than one ASes to advertise the same set of IP prefixes, the holder must issue multiple ROAs, one for each AS number. However, at present there are no mandatory requirements describing that the address space holders must issue a separate ROA for each IP prefix or a ROA containing multiple IP Sprefixes.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Problem Statement

For a Certification Authority (CA) issuing ROAs containing multiple IP prefixes, adding or deleting one <AS, IP_Prefix> pair causes the (single) ROA for an AS to be withdrawn and reissued. All IP prefixes for an AS share the same validation state and then this may affect the stability and security of RPKI.

By default, ROAs have an extended validity period. Resource changes can happen at any time during this validity period. A certificate change can affect all ROAs using IP prefixes from the issuing certificate. CAs should carefully coordinate ROA updates with resource certificate updates. A CA can automate this process if a single entity manages both the parent CA and the CA issuing the ROAs (scenario D [[RFC8211] section 3]). However, in other deployment scenarios, this coordination becomes more complex. Furthermore, for the ROA containing multiple IP prefixes, the IP prefixes share the same expiry configuration. If the ROA is not reissued timely, the whole set of IP prefixes will be affected after expiry.

Using multiple ROA objects with single IP prefix also allows a CA to affect routing over time based on certificate expiry. For example, a prefix could be allowed to be originated from an AS only for a specific period of time, such as some IP prefix was leased out temporarily.

4. Suggestions

The following suggestions should be considered during the process of ROA issurance:

1) It's the most important to guarantee the stability and security of RPKI, and it is recommended to include a single IP prefix in each ROA in default.

2) In some special scenarios, where the resource is very stable or a CA has operational problems producing increased number of individual ROAs, multiple IP prefixes may be aggregated in one ROA.

5. Security Considerations

This memo does not give rise to additional security risks.

6. IANA Considerations

This document does not request any IANA action.

7. Acknowledgements

The authors would like to thanks the valuable comments made by members of sidrops WG and the list will be updated later.

This work was supported by the Beijing Nova Program of Science and Technology under grant Z191100001119113.

This document was produced using the xml2rfc tool [RFC2629].

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>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8211] Kent, S. and D. Ma, "Adverse Actions by a Certification Authority (CA) or Repository Manager in the Resource Public Key Infrastructure (RPKI)", RFC 8211, DOI 10.17487/RFC8211, September 2017, <https://www.rfc-editor.org/info/rfc8211>.

8.2. Informative References

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, DOI 10.17487/RFC2629, June 1999, <https://www.rfc-editor.org/info/rfc2629>.

Appendix A. ROA Analysis

In order to illustrate the situations of the current ROA database, the following analysis is made.

The total number of ROAs	The number of ROAs with a single prefix	The number of ROAs with multiple prefixes
117898	92742	25156

Figure 1: Statistical results of global ROAs

As shown in Figure. 1, by July 20th 2022, the total number of ROA objects issued is about 117898. Based on the further analysis on these ROA objects, it is found that the number of ROAs containing only one prefix is about 92742 (78.66% of all ROA objects), and the number of ROAs containing two or more prefixes is about 25156 (21.34% of all ROA objects).

In the 25156 ROA objects which each one contains two or more prefixes, the number of IP address prefixes are calculated and analyzed. The statistical results are shown in Figure. 2.

The number of prefixes	The number of ROAs	The median number of prefixes in ROA
271822	25156	3

Figure 2: Statistical results of the ROAs with multiple prefixes

As described in Figure. 2, there are 271822 IP address prefixes in the 25156 ROA objects. And the median number of prefixes in ROA is 3. In addition, four types of ROAs are analyzed and calculated within the 25156 ROAs: ROAs each contains 2-10/11-50/51-100/>100 IP address prefixes. The statistical results are presented in Figure. 3.

ROA types	ROA with 2-10 prefixes	ROA with 11-50 prefixes	ROA with 51-100 prefixes	ROA with >100 prefixes	Total number
The number of ROAs	21461	3042	343	310	25156
The ratio of ROAs	85.31%	12.09%	1.36%	1.23%	100%
The number of prefixes	78677	62156	23676	107313	271822
The ratio of prefixes	28.94%	22.87%	8.71%	39.48%	100%

Figure 3: Statistical results of four types of ROAs

As shown in Figure. 3, taking the first type of ROA as an example, there are 21461 ROAs (85.31% of the 25156 ROA objects) containing 2-10 IP address prefixes, and the total number of IP prefixes in these 21461 ROAs is 78677 (28.94% of the 271822 prefixes). It shows that the address space holders tend to issue each ROA object with multiple IP prefixes (more than 95% of ROAs containing 2-50 prefixes).

The longest and shortest validity periods of a single ROA is 28854 days and 2 days. In addition, the median validity period of ROA is 429 days.

Authors' Addresses

Zhiwei Yan
CNNIC
No.4 South 4th Street, Zhongguancun
Beijing, 100190
P.R. China
Email: yanzhiwei@cnnic.cn

Randy Bush
Internet Initiative Japan
Email: randy@psg.com

Guanggang Geng
Jinan University
No.601, West Huangpu Avenue
Guangzhou
510632
China
Email: gggeng@jnu.edu.cn

Ties de Kock
RIPE NCC
Stationsplein 11
Amsterdam
Email: tdekock@ripe.net