Workgroup: Network Working Group
Internet-Draft:
draft-ymbk-sidrops-rov-no-rr-01
Published: 12 November 2021
Intended Status: Informational
Expires: 16 May 2022
Authors: R. Bush
IIJ Research Lab & Arrcus, Inc.
K. Patel
Arrcus, Inc.
P. Smith
PFS Internet Development Pty Ltd
M. Tinka
SEACOM

RPKI Route Origin Validation Without Route Refresh

Abstract

A BGP Speaker performing RPKI-based Route Origin Validation should not issue Route Refresh to its neighbors when receiving new VRPs. A method for avoiding doing so is described.

Requirements Language

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.

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 16 May 2022.

Copyright Notice

Table of Contents

1. Introduction

Memory constraints in early routers caused classic [RFC4271] BGP implementations to not keep a full Adj-RIB-In (Sec. 1.1). When doing RPKI-based Route Origin Validation ([RFC6811] and [RFC8481]), if such a BGP speaker receives new ROAs/VRPs, it might not have kept paths previously marked as Invalid. Such an implementation must then request a Route Refresh [RFC7313] from its neighbors to recover the paths which might be covered by these new VRPs. This will be perceived as rude by those neighbors as it passes a serious resource burden on to them. This document recommends implementations keep but mark Invalidated paths so the Route Refresh is no longer needed.

2. Related Work

It is assumed that the reader understands BGP, [RFC4271] and Route Refresh [RFC7313], the RPKI [RFC6480], Route Origin Authorizations (ROAs), [RFC6482], The Resource Public Key Infrastructure (RPKI) to Router Protocol [I-D.ietf-sidrops-8210bis], RPKI-based Prefix Validation, [RFC6811], and Origin Validation Clarifications, [RFC8481].

3. Operational Recommendations

Routers MUST either keep the full Adj-RIB-In or implement this specification.

Operators deploying ROV SHOULD ensure that the router implementation is not causing unnecessary Route Refresh requests to neighbors.

If the router does not implement the recommendations here, the operator SHOULD enable the vendor's knob to keep the full Adj-RIB-In, sometimes referred to as "soft reconfiguration inbound". The operator should then ensure that this stops unnecessary Route Refresh requests to neighbors.

If the router has insufficient resources to support this, it MUST not be used for Route Origin Validation.

4. Security Considerations

This document describes a denial of service Route Origin Validation may place on a BGP neighbor, and describes how it may be ameliorated.

Otherwise, this document adds no additional security considerations to those already described by the referenced documents.

5. IANA Considerations

None

6. References

6.1. Normative References

[I-D.ietf-sidrops-8210bis] Bush, R. and R. Austein, "The Resource Public Key Infrastructure (RPKI) to Router Protocol, Version 2", Work in Progress, Internet-Draft, draft-ietf-sidrops-8210bis-03, 15 August 2021, <https://www.ietf.org/archive/id/draft-ietf-sidrops-8210bis-03.txt>.

[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>.

[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>.

[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>.

[RFC7313] Patel, K., Chen, E., and B. Venkatachalapathy, "Enhanced Route Refresh Capability for BGP-4", RFC 7313, DOI 10.17487/RFC7313, July 2014, <https://www.rfc-editor.org/info/rfc7313>.

[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>.

[RFC8481] Bush, R., "Clarifications to BGP Origin Validation Based on Resource Public Key Infrastructure (RPKI)", RFC 8481, DOI 10.17487/RFC8481, September 2018, <https://www.rfc-editor.org/info/rfc8481>.

6.2. Informative References

[RFC6480] Lepinski, M. and S. Kent, "An Infrastructure to Support Secure Internet Routing", RFC 6480, DOI 10.17487/RFC6480, February 2012, <https://www.rfc-editor.org/info/rfc6480>.

Authors' Addresses

Randy Bush
IIJ Research Lab & Arrcus, Inc.
1856 SW Edgewood Dr
Portland, Oregon 97210
United States of America

Email: randy@psg.com

Keyur Patel
Arrcus, Inc.
2077 Gateway Place, Suite #400
San Jose, CA 95119
United States of America

Email: keyur@arrcus.com

Philip Smith
PFS Internet Development Pty Ltd
PO Box 1908
Milton QLD 4064
Australia

Email: pfsinoz@gmail.com

Mark Tinka
SEACOM
Building 7, Design Quarter District, Leslie Avenue, Magaliessig
Fourways, Gauteng
2196
South Africa

Email: mark@tinka.africa