Stream:	Internet Engineering Task Force (IETF)
RFC:	8893
Updates:	6811
Category:	Standards Track
Published:	September 2020
ISSN:	2070-1721
Authors:	R. Bush	R. Volk	J. Heitz
---	---	---	---
	Internet Initiative Japan & Arrcus		*Cisco*

RFC 8893
Resource Public Key Infrastructure (RPKI) Origin Validation for BGP Export

Abstract

A BGP speaker may perform Resource Public Key Infrastructure (RPKI) origin validation not only on routes received from BGP neighbors and routes that are redistributed from other routing protocols, but also on routes it sends to BGP neighbors. For egress policy, it is important that the classification use the 'effective origin AS' of the processed route, which may specifically be altered by the commonly available knobs, such as removing private ASes, confederation handling, and other modifications of the origin AS. This document updates RFC 6811.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8893.

Copyright Notice

Table of Contents

1. Introduction

This document does not change the protocol or semantics of [RFC6811], BGP prefix origin validation. It highlights an important use case of origin validation in external BGP (eBGP) egress policies, explaining specifics of correct implementation in this context.

The term 'effective origin AS' as used in this document refers to the Route Origin Autonomous System Number (ASN) [RFC6811] of the UPDATE to be sent to neighboring BGP speakers.

The effective origin AS of a BGP UPDATE is decided by configuration and outbound policy of the BGP speaker. A validating BGP speaker **MUST** apply Route Origin Validation policy semantics (see Section 2 of [RFC6811] and Section 4 of [RFC8481]) after applying any egress configuration and policy.

This effective origin AS of the announcement might be affected by removal of private ASes, confederation [RFC5065], migration [RFC7705], etc. Any AS_PATH modifications resulting in effective origin AS change **MUST** be taken into account.

This document updates [RFC6811] by clarifying that implementations must use the effective origin AS to determine the Origin Validation state when applying egress policy.

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.

2. Suggested Reading

It is assumed that the reader understands BGP [RFC4271], the RPKI [RFC6480], Route Origin Authorizations (ROAs) [RFC6482], RPKI-based Prefix Validation [RFC6811], and Origin Validation Clarifications [RFC8481].

3. Egress Processing

BGP implementations supporting RPKI-based origin validation **MUST** provide the same policy configuration primitives for decisions based on the validation state available for use in ingress, redistribution, and egress policies. When applied to egress policy, validation state **MUST** be determined using the effective origin AS of the route as it will (or would) be announced to the peer. The effective origin AS may differ from that of the route in the RIB due to commonly available knobs, such as removal of private ASes, AS path manipulation, confederation handling, etc.

Egress policy handling can provide more robust protection for outbound eBGP than relying solely on ingress (iBGP, eBGP, connected, static, etc.) redistribution being configured and working correctly -- i.e., better support for the robustness principle.

4. Operational Considerations

Configurations may have a complex policy where the effective origin AS may not be easily determined before the outbound policies have been run. It **SHOULD** be possible to specify a selective origin validation policy to be applied after any existing non-validating outbound policies.

An implementation **SHOULD** be able to list announcements that were not sent to a peer, e.g., because they were marked Invalid, as long as the router still has them in memory.

5. Security Considerations

This document does not create security considerations beyond those of [RFC6811] and [RFC8481]. By facilitating more correct validation, it attempts to improve BGP reliability.

6. IANA Considerations

This document has no IANA actions.

7. References

7.1. 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>.

[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>.

[RFC5065] Traina, P., McPherson, D., and J. Scudder, "Autonomous System Confederations for BGP", RFC 5065, DOI 10.17487/RFC5065, August 2007, <https://www.rfc-editor.org/info/rfc5065>.

[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>.

[RFC7705] George, W. and S. Amante, "Autonomous System Migration Mechanisms and Their Effects on the BGP AS_PATH Attribute", RFC 7705, DOI 10.17487/RFC7705, November 2015, <https://www.rfc-editor.org/info/rfc7705>.

[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>.

7.2. 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>.

Acknowledgments

Thanks to reviews and comments from Linda Dunbar, Nick Hilliard, Benjamin Kaduk, Chris Morrow, Keyur Patel, Alvaro Retana, Job Snijders, Robert Sparks, and Robert Wilton.

Authors' Addresses

Randy Bush
Internet Initiative Japan & Arrcus
5147 Crystal Springs
Bainbridge Island, WA 98110
United States of America
Email: randy@psg.com

Rüdiger Volk
Email: ietf@rewvolk.de

Jakob Heitz
Cisco
170 West Tasman Drive
San Jose, CA 95134
United States of America
Email: jheitz@cisco.com