Internet Engineering Task Force (IETF)
Internet-Draft
Updates: 6811, 8097 (if approved)
Intended status: Standards Track
Expires: July 19, 2021

O. Borchert
D. Montgomery
USA NIST

January 15, 2021

RPKI Route Origin Validation State Unverified
draft-borchert-sidrops-rpki-state-unverified-04

Abstract

In case operators decide not to evaluate BGP route prefixes according to RPKI route origin validation (ROV), none of the available states as specified in RFC 6811 do properly represent this decision. This document introduces "Unverified" as well-defined validation state which allows to properly identify route prefixes as not evaluated according to RPKI route origin validation.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 3
1.1. Terminology 3
2. Suggested Reading 3
3. Initializing route prefixes 3
3.1. Update to RFC 6811 4
3.2. Update to RFC 8097 4
3. Usage Considerations 5
4. Security Considerations 5
5. IANA Considerations 5
6. References 6
6.1. Normative References 6
8.2. Informative References 6
Acknowledgements 7
Authors' Addresses 7

1. Introduction

Prefix origin validation provides well-defined validation states. Though, there are instances in which no evaluation of a route prefix is performed, not through RPKI route origin validation [RFC6811], signaling via the extended community string as specified in [RFC8097], or operator configuration. In these circumstances RFC 6811 specifies the implementation SHOULD initialize the validation state of such route to "NotFound". Here, the absence of a well-defined validation state for a route prefix not evaluated, requires the usage of a state otherwise reserved as outcome of the evaluation of such. This "waters" down the meaning of the used state. The specification of a proper validation state that allows identifying non-evaluated routes, becomes of essence once an operator decides to write policies on the validation state "NotFound". A route prefix labeled "NotFound" cannot be considered same as an unverified route prefix.

Hence, this document updates RFC 6811 and RFC 8097 by adding the proposed validation state "Unverified".

1.1. 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.

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], BGP Prefix Origin Validation State Extended Community [RFC8097], Clarifications to BGP Origin Validation Based on Resource Public Key Infrastructure (RPKI) [RFC8481]

3. Initializing route prefixes

This document introduces the validation state "Unverified" to be used for route prefixes that are not evaluated through either operator configuration, RPKI route origin validation, or other means such as receiving a signaled validation state via the extended community string. To allow proper initialization the following state is introduced:

- Unverified: Specifies the state of a route prefix on which no evaluation has been performed.

3.1. Update to RFC 6811

RFC 6811 specifies that:

> If validation is not performed on a Route, the implementation SHOULD initialize the validation state of such a route to "NotFound".

This document specifies that:

If no evaluation of a route prefix is performed in any form, the implementation MUST initialize the validation state of such a route to "Unverified".

This removes the necessity to initialize the route with any of the states "Valid", "Invalid", or "NotFound" and therefore does not "water-down" the meaning of such.

3.2. Update to RFC 8097

As specified in RFC 8097:

> If the router is configured to support the extensions defined in this document" - (RFC 8097) - ", it SHOULD attach the origin validation state extended community to BGP UPDATE messages sent to IBGP peers by mapping the computed validation state in the last octet of the extended community.

The missing part here is what to do with route prefixes not evaluated and no validation state was assigned. At this point the only solution is to omit the extended community for such routes. If the usage of the extended community would have been negotiated during the BGP OPEN MESSAGE the receiver would be able to determine that the sender did not evaluate the route in any form. But this is not the case, so a receiver does not know if the sender is RPKI capable and chose not to attach the origin validation state to the BGP UPDATE or the route did not have any validation state assigned.

Hence, this document specifies for all routes that are labeled as "Unverified" to attach the "unverified" state extended community to BGP UPDATE messages send to IBGP peers by mapping the computed validation state in the last octet of the extended community.

AS specified in the table below, this document adds the value "unverified = 3" to the list of acceptable values.

The value on the protocol

Value	Meaning
0	Lookup result = "valid"
1	Lookup result = "not found"
2	Lookup result = "invalid"
3	Lookup result = "unverified"

3. Usage Considerations

The well-defined validation state "Unverified" allows to distinguish between evaluated routes and non-evaluated routes. This allows the operator to create policies to treat such route prefixes different from route prefixes labeled with one of the validation states "Valid", "NotFound", or "Invalid".

4. Security Considerations

This document introduces no new security concerns beyond what is described in [RFC6811] and [RFC8097]

5. IANA Considerations

This document has no IANA actions.

6. References

6.1. 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>.

[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>.

[RFC8097] Mohapatra, P., Patel, K., Scudder, J., Ward, D., and R. Bush, "BGP Prefix Origin Validation State Extended Community", RFC 8097, DOI 10.17487/RFC8097, March 2017, <https://www.rfc-editor.org/info/rfc8097>.

[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>.

8.2. Informative References

[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>.

[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>.

[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>.

[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>.

Acknowledgements

The authors would like to acknowledge the valuable review and suggestions from K. Sriram on this document.

Authors' Addresses

Oliver Borchert
National Institute of Standards and Technology (NIST)
100 Bureau Drive
Gaithersburg, MD 20899
United States of America

Email: oliver.borchert@nist.gov

Doug Montgomery
National Institute of Standards and Technology (NIST)
100 Bureau Drive
Gaithersburg, MD 20899
United States of America

Email: dougm@nist.gov