Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 4, 2018

R. Bush
Internet Initiative Japan

July 3, 2017

Origin Validation Clarifications
draft-ymbk-sidrops-ov-clarify-00

Abstract

Deployment of RPKI-based BGP origin validation is hampered by, among other things, vendor mis-implementions in two critical areas, which routes are validated and whether policy is applied when not specified by configuration. This document is meant to clarify possible misunderstandings causing those mis-implementatons.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [RFC2119] only when they appear in all upper case. They may also appear in lower or mixed case as English words, without normative meaning.

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 http://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 January 4, 2018.

Copyright Notice

1. Introduction

Deployment of RPKI-based BGP origin validation is hampered by, among other things, vendor mis-implementions in two critical areas, which routes are validated and whether policy is applied when not specified by configuration. This document is meant to clarify possible misunderstandings causing those mis-implementations.

When a route is distributed into BGP, origin validation marks the announcement as NotFound, Valid, or Invalid per [RFC6811]. Operational testing has shown that the specifications of that RFC must be unclear. This document attempts to clarify two areas seeming to cause confusion.

The implementation issues seem not to be about how to validate, i.e., how to decide if a route is NotFound, Valid, or Invalid. The issues seem to be which routes to mark and whether to apply policy without operator configuration.

2. Suggested Reading

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

3. Mark ALL Prefixes

An operator should not have to hear from their neighbor that they announced an Invalid route. Their routers should tell them before announcing the Invalid route to a neighbor. For this reason, [RFC6811] says

"When a BGP speaker receives an UPDATE from a neighbor, it SHOULD perform a lookup as described above for each of the Routes in the UPDATE message. The lookup SHOULD also be applied to routes that are redistributed into BGP from another source, such as another protocol or a locally defined static route."

[RFC6811] goes on to say "An implementation MAY provide configuration options to control which routes the lookup is applied to." In the absence of the operator applying such policy, ALL routes in BGP MUST be marked.

This means that, on a router, all routes in BGP, absent operator configuration otherwise, MUST have been marked because they were either received via BGP (whether eBGP or iBGP), redistributed from an IGP, static, or directly connected, or any other distribution into BGP.

4. Marking not Acting

Once routes are marked, the operator should be in complete control of any policy applied based the markings. Absent operator configuration, policy MUST NOT be applied.

Automatic policy actions such as those described in [RFC8097], BGP Prefix Origin Validation State Extended Community, MUST NOT be carried out or otherwise applied unless specifically configured by the operator.

5. Security Considerations

This document does not create security considerations beyond those of [RFC6811].

6. IANA Considerations

This document has no IANA Considerations.

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, <http://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, <http://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, <http://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, <http://www.rfc-editor.org/info/rfc8097>.

7.2. 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, <http://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, <http://www.rfc-editor.org/info/rfc6480>.

Author’s Address

Randy Bush
Internet Initiative Japan
5147 Crystal Springs
Bainbridge Island, Washington 98110
US

Email: randy@psg.com