Internet Engineering Task Force (IETF)
Request for Comments: 9674
Updates: 8182
Category: Standards Track
ISSN: 2070-1721

J. Snijders
Fastly

December 2024

Same-Origin Policy for the RPKI Repository Delta Protocol (RRDP)

Abstract

This document describes a Same-Origin Policy (SOP) requirement for Resource Public Key Infrastructure (RPKI) Repository Delta Protocol (RRDP) servers and clients. Application of a SOP in RRDP client/server communication isolates resources such as Delta and Snapshot files from different Repository Servers, reducing possible attack vectors. This document updates RFC 8182.

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/rfc9674.

Table of Contents

Author’s Address

1. Introduction

This document specifies a Same-Origin Policy (SOP) requirement for RPKI Repository Delta Protocol (RRDP) servers and clients. The SOP concept is a security mechanism to restrict how a document loaded from one origin can cause interaction with resources from another origin. See [RFC6454] for an overview of the concept of an "origin". Application of a SOP in RRDP client/server communication isolates resources such as Delta and Snapshot files from different Repository Servers, reducing possible attack vectors. Another way to avoid undesirable implications (as described in Section 2) would be for a future version of RRDP to use relative URIs instead of absolute URIs. This document updates [RFC8182].

1.1. 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.

2. Implications of Cross-Origin Resource Requests in RRDP

The first RRDP specification did not explicitly disallow ’cross-origin’ URI references from the Update Notification file (Section 3.5.1 of [RFC8182]) towards Delta (Section 3.5.3 of [RFC8182]) and Snapshot (Section 3.5.2 of [RFC8182]) files, and it was silent on the topic of HTTP Redirection (Section 15.4 of [RFC9110]).

The implication of cross-origin references in Update Notification files is that one Repository Server can reference RRDP resources on another Repository Server and in doing so inappropriately increase the resource consumption for both RRDP clients and the referenced Repository Server. An adversary could also employ cross-origin HTTP Redirects towards other Repository Servers, causing similar undesirable behavior.

3. Changes to RFC 8182

To overcome the issue described in Section 2, RRDP Repository Servers and Clients MUST apply a Same-Origin Policy to both the URIs referenced in an Update Notification File and any HTTP Redirects.

3.1. New Requirements for RRDP Repository Servers

The following checklist items are added to Section 3.5.1.3 of [RFC8182]:

NEW

| * The "uri" attribute in the snapshot element and optional delta elements MUST be part of the same origin (i.e., represent the same principal), meaning referenced URIs MUST have the same scheme, host, and port as the URI for the Update Notification File specified in the referring RRDP SIA AccessDescription.
|
| * The Repository Server MUST NOT respond with HTTP Redirects towards locations with an origin different from the origin of the Update Notification File specified in the referring RRDP SIA AccessDescription.

3.2. New Requirements for Relying Parties Using RRDP

The following adds to Section 3.4.1 of [RFC8182]:

NEW

| * The Relying Party MUST verify whether the "uri" attributes in
| the Update Notification File are of the same origin as the
| Update Notification File itself. If this verification fails,
| the file MUST be rejected and RRDP cannot be used; see
| Section 3.4.5 for considerations. Implementations SHOULD log a
| message when cross-origin referrals are detected.
|
| * The Relying Party MUST NOT follow HTTP Redirection that results
| from attempts to download Update Notification, Delta, and
| Snapshot files if the target origin is different from the
| origin of the Update Notification File specified in the
| referring RRDP SIA AccessDescription. If this verification
| fails, the RRDP session MUST be rejected and RRDP cannot be
| used; see Section 3.4.5 for considerations. Implementations
| SHOULD log a message when cross-origin redirects are detected.

4. Deployability in the Internet’s Current RPKI

Analyzing the [rpkiviews] archives for the period from April to September 2024, only one RRDP server (reached following the Trust Anchor Locators (TALs) of the five Regional Internet Registries) employed a same-origin HTTP redirect. In the period October 2021 - October 2024 no RRDP Repository Servers were observed that employed cross-origin URIs in Update Notification Files.

This means that imposing a requirement for the application of a Same-Origin Policy does not cause any existing commonly used RRDP Repository Server operations to become non-compliant.

5. Security Considerations

This document addresses an oversight in the original RRDP specification: Cross-origin requests are detrimental as they allow one repository operator to increase resource consumption for other repository operators and RRDP clients.

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>.

[RFC6454] Barth, A., "The Web Origin Concept", RFC 6454, DOI 10.17487/RFC6454, December 2011, <https://www.rfc-editor.org/info/rfc6454>.

[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>.

[RFC8182] Bruijnzeels, T., Muravskiy, O., Weber, B., and R. Austein, "The RPKI Repository Delta Protocol (RRDP)", RFC 8182, DOI 10.17487/RFC8182, July 2017, <https://www.rfc-editor.org/info/rfc8182>.

[RFC9110] Fielding, R., Ed., Nottingham, M., Ed., and J. Reschke, Ed., "HTTP Semantics", STD 97, RFC 9110, DOI 10.17487/RFC9110, June 2022, <https://www.rfc-editor.org/info/rfc9110>.

7.2. Informative References

[rpkiviews] Snijders, J., "rpkiviews", <https://www.rpkiviews.org>.

Acknowledgements

The author wishes to thank Theo Buehler, Claudio Jeker, Alberto Leiva, Tim Bruijnzeels, Ties de Kock, Martin Hoffmann, and Mikhail Puzanov for their helpful feedback, comments, and implementation work. The author wishes to thank Keyur Patel, Meral Shirazipour, Niclas Comstedt, Dan Harkins, Erik Kline, Roman Danyliw, and ric Vyncke for their review.

Author’s Address

Job Snijders
Fastly
Amsterdam
Netherlands
Email: job@fastly.com