Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 17, 2018

R. Shoemaker
ISRG

September 13, 2017

Certification Authority Authorization (CAA) Validation for IP Addresses

draft-shoemaker-caa-ip-01

Abstract

The Certification Authority Authorization (CAA) RFC specifies a method for users to restrict which Certificate Authorities (CAs) are authorized to issue certificates for their DNS domain names. This document extends that specification to provide a method for holders of IP addresses to do the same.

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 March 17, 2018.

Copyright Notice

Table of Contents

1. Introduction

This document describes an extension to RFC 6844 [RFC6844] which allows for the use of Certification Authority Authorization DNS Records to be used to restrict issuance of certificates to IP addresses instead of just DNS names. This is done by defining a new lookup mechanism for IPv4 and IPv6 addresses as previously a mechanism only existed for DNS names.

2. Terminology

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [RFC2119].

3. Mechanism

Before issuing a certificate containing a IP address a compliant CA MUST check for the relevant CAA Resource Record set. If such a record set exists a CA MUST NOT issue a certificate unless the records in the set are consistent with the request and the policies of the CA.

A certificate request MAY specify more than one IP address in which case CAs MUST verify the CA Resource Record set for all the IP addresses specified in the request.

As defined in RFC 2818 [RFC2818] IP addresses in certificates must match exactly with the requested URI so CAs MUST NOT consider CAA records with the "issuewild" tag to be part of the relevant Resource Record set for a IP address.

Unlike the mechanism defined in RFC 6844 [RFC6844] this mechanism doesn't involve climbing the DNS tree and only requires querying a single DNS name. The relevant Resource Record set for a given IP address is found by querying the reverse mapping zone for the IP for CAA records.

Given a certificate request containing the IPv6 address "2001:db8::1" the relevant query for the reverse mapping within the IP6.ARPA [RFC3596] zone would be:

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.d.0.1.0.0.2.ip6.arpa. IN CAA

And for a request containing the IPv4 address "192.0.2.1" the relevant query for the reverse mapping within the IN-ADDR.ARPA [RFC1034] zone would be:

1.2.0.192.in-addr.arpa. IN CAA

When doing queries CAs SHOULD either use a resolver that chases CNAME records or manually chase CNAMEs themselves in order to allow for zone delegations [RFC2317].

4. IANA Considerations

4.1. Certification Authority Restriction Properties

Change the contents of the Meaning column for the "issue" Tag to say "Authorization Entry by Domain or IP address" and add "draft-shoemaker-caa-ip" to the References column.

5. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987, <https://www.rfc-editor.org/info/rfc1034>.

[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>.

[RFC2317] Eidnes, H., de Groot, G., and P. Vixie, "Classless IN-ADDR.ARPA delegation", BCP 20, RFC 2317, DOI 10.17487/RFC2317, March 1998, <https://www.rfc-editor.org/info/rfc2317>.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, DOI 10.17487/RFC2818, May 2000, <https://www.rfc-editor.org/info/rfc2818>.

[RFC3596] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, "DNS Extensions to Support IP Version 6", STD 88, RFC 3596, DOI 10.17487/RFC3596, October 2003, <https://www.rfc-editor.org/info/rfc3596>.

[RFC6844] Hallam-Baker, P. and R. Stradling, "DNS Certification Authority Authorization (CAA) Resource Record", RFC 6844, DOI 10.17487/RFC6844, January 2013, <https://www.rfc-editor.org/info/rfc6844>.

Author's Address

Roland Bracewell Shoemaker
ISRG

Email: roland@letsencrypt.org