RTCWEB
Internet-Draft
Intended status: Informational
Expires: January 9, 2020

J. Uberti
J. de Borst
Q. Wang
Google
Y. Fablet
Apple Inc.
July 08, 2019

WebRTC IP Address Handling Extensions for Multicast DNS
draft-uberti-rtcweb-ip-handling-ex-mdns-01

Abstract

This document extends the previous WebRTC IP Address Handling Requirements with new modes that make use of Multicast DNS ICE candidates, and updates the recommendations accordingly.

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 https://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 9, 2020.

Copyright Notice

Copyright (c) 2019 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 (https://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 2
2. Terminology 2
3. New Modes 2
3.1. Mode 2.1 3
3.2. Mode 2.2 3
4. Analysis 3
5. Additional Applications 3
6. Security Considerations 3
7. IANA Considerations 4
8. References 4
8.1. Normative References 4
8.2. Informative References 4
Authors' Addresses 4

1. Introduction

[IPHandling] describes the privacy problems associated with exposing IP addresses to web applications, but admits that there is no solution to the issue of exposing private IP addresses that does not carry a corresponding impact on connectivity.

[mDNSCandidates] introduces a new technique based on Multicast DNS (mDNS) that obscures private IP addresses with mDNS names. This solves the privacy issues associated with exposing local IP addresses, and mitigates most of the aforementioned connectivity impact.

This document extends the set of modes defined in [IPHandling] with new options based on the mDNS technique. Different choices are provided, each with their own benefits and drawbacks.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

3. New Modes

Using the mDNS technique, we define two new modes, namely Mode 2.1 and 2.2. These modes are identical to Mode 2 from [IPHandling], but the technique from [mDNSCandidates] is used to protect the selected private IP addresses. Accordingly, the privacy guidelines outlined

in [mDNSCandidates], Section 5 MUST be followed in each new mode in order to prevent accidental disclosure of a private IP address.

3.1. Mode 2.1

The local IPv4 address associated with the preferred interface MUST be replaced with a mDNS name, as described in [mDNSCandidates], Section 3.1. Any local IPv6 addresses associated with the preferred interface MUST also be replaced with mDNS names, unless they are [RFC4941] privacy-preserving addresses.

3.2. Mode 2.2

All local IPv4 and IPv6 addresses MUST be replaced with mDNS names, as described in [mDNSCandidates], Section 3.1.

4. Analysis

The only difference between Mode 2.1 and Mode 2.2 is how [RFC4941] addresses are handled. In either case, a direct connection is possible if the mDNS addresses created for the local IP addresses can be resolved. However, when mDNS fails, either because it is disabled on the network, or the endpoints are not on the same segment, Mode 2.1 may allow a direct connection where Mode 2.2 does not.

The exact impact on applications needs to be determined experimentally. This document will be updated with a specific recommendation once this information is known.

5. Additional Applications

The mDNS technique may also have value even when all network interfaces are used by the ICE agent, i.e., in Mode 1 from [IPHandling], by minimizing the amount of information regarding the local network that is disclosed to the remote peer. Accordingly, a future update of this document may define additional modes that apply the mDNS technique to Mode 1. This is an area for further study.

6. Security Considerations

The modes defined here, on their own, present no new security considerations. Considerations for the mDNS technique are detailed in [mDNSCandidates], Section 6.

7. IANA Considerations

This document requires no actions from IANA.

8. References

8.1. 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>.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007, <https://www.rfc-editor.org/info/rfc4941>.

8.2. Informative References

[IPHandling] Shieh, G., "WebRTC IP Address Handling Requirements", April 2018, <https://tools.ietf.org/html/draft-ietf-rtcweb-ip-handling>.

[mDNSCandidates] Wang, Q., "Using Multicast DNS to protect privacy when exposing ICE candidates", October 2018, <https://tools.ietf.org/html/draft-ietf-rtcweb-mdns-ice-candidates>.

Authors' Addresses

Justin Uberti
Google

Email: juberti@google.com

Jeroen de Borst
Google

Email: jeroendb@google.com

Qingsi Wang
Google

Email: qingsi@google.com

Youenn Fablet
Apple Inc.

Email: youenn@apple.com