☆ Starred by 1 user

Owner:	hta@chromium.org
CC:	adetaylor@chromium.org orphis@chromium.org
Status:	Fixed *(Closed)*
Components:	Blink>WebRTC>Network
Modified:	Sep 28, 2020
Backlog-Rank:	----
Editors:	----
EstimatedDays:	----
NextAction:	----
OS:	Linux, Android, Windows, Chrome, Mac
Pri:	2
Type:	Bug-Security

reward-0
Security_Severity-Low
Security_Impact-Stable
allpublic
CVE_description-submitted
M-85
Release-0-M85
CVE-2020-6570

Issue 1084699: [WebRTC] Remote ICE Candidate Hostname Lookup Privacy Issue

Reported by a_deleted_user on Tue, May 19, 2020, 5:27 PM EDT

Code

VULNERABILITY DETAILS
When establishing an ICE connection via WebRTC, the remote ICE agent may send an ICE candidate to the local ICE agent containing a hostname (rather than an IP address). Currently, WebRTC's behavior is to resolve these hostnames via a DNS lookup. This action allows the remote ICE agent to cause the local ICE agent to do a DNS lookup to a domain under the remote ICE agent's control.

Using this, the remote host may cause the local host's DNS server to connect to an authoritative DNS server under the remote host's control, thus revealing the local host's DNS server to the remote host. In the context of a video call, this means a caller could use this mechanism to learn the IP address of the DNS server of the other party even if they are intentionally routing all traffic through proxy servers. If the DNS server supports EDNS Client Subnet (ECS), the caller could also learn a resolver-defined number of bits of the other party's IP address. Google Public DNS, for example, supports ECS, exposing 24 bit of a client IP address.

One possible solution is to allow WebRTC to be configured to control whether mDNS/DNS queries are sent for remote ICE candidates with hostnames. Changing this behavior is a simple fix, but different clients may want different behavior. Some may wish to only use IP addresses and do no DNS or mDNS lookups. Others may wish to enable both. It seems like the best default would be to enable mDNS queries but not DNS queries, to avoid any IP leak issue while retaining the mDNS connectivity defined by https://tools.ietf.org/html/draft-ietf-rtcweb-mdns-ice-candidates-04). The included patch allows for such configurable behavior.

This issue was reported to Signal by Tenable Inc. A different fix was made by Signal in our WebRTC fork here:
https://github.com/signalapp/webrtc. Here is the relevant diff:
https://github.com/signalapp/webrtc/compare/402f9f2c5d74cf24496a795524a6d5aea16fb71b..60f340669034d0b59fe4ccab0239e4f8d5751c56. Unlike the included patch, it is not configurable, opting for the simple approach of disabling both DNS and mDNS queries.

Tenable has indicated they are likely to make this public later in the week, possibly on Friday (May 22).

VERSION
The code to resolve hostnames in ICE candidates was introduced in WebRTC commit 6fcdc2f70815601861f7a718c67490a5f14f1e1b.

REPRODUCTION CASE
- An attacker sets up an authoritative DNS server for a domain they control - i.e. evil.com
- The attacker tries to establish a ICE connection with a victim, specifying evil.com in an ICE candidate
- Upon receipt of the ICE candidate, the victim tries to resolve the IP address for evil.com
- The attacker learns the victim’s DNS server
- If the DNS server supports ECS, the attacker learns parts of the victim’s IP address

CREDIT INFORMATION
This issue was reported to Signal by Tenable Inc. via bughunters@tenable.com.
Signal authored the proposed patch.

configurable-ice-mdns.patch
18.0 KB View Download

Comment 1 by kenrb@chromium.org on Tue, May 19, 2020, 6:06 PM EDT Project Member

Components: Blink>WebRTC>Network

Thanks for the report.

This would be low severity by our security guidelines.

Tagging the relevant WebRTC component for assessment.

Comment 2 by guidou@chromium.org on Wed, May 20, 2020, 1:32 AM EDT Project Member

Status: Assigned (was: Unconfirmed)
Owner: hta@chromium.org
Cc: adetaylor@chromium.org

hta@: Can you take a look?

Comment 3 by hta@chromium.org on Wed, May 20, 2020, 4:39 AM EDT Project Member

DNS candidates have been an active topic of discussion in the IETF (last round triggered by, but not directly related to, the mDNS extension).
The old guidance for use of DNS candidates is here: https://www.rfc-editor.org/rfc/rfc5245.html#section-15.1; there are situations where this isn't completely clear - but I don't think we ever considered the lookup of DNS entries to be a risk.

There are many other ways to cause a DNS lookup to happen in the Web (including the Fetch algorithm), so it's not clear that configuring this to "off" would bring any increased security.

Suggest marking this as "wontfix" unless a compelling argument can be made why this behavior is an actual vulnerability increase.

Comment 4 by guidou@chromium.org on Thu, May 21, 2020, 5:47 AM EDT Project Member

Status: WontFix (was: Assigned)

Closing as per #c3

Comment 5 by guidou@chromium.org on Thu, May 21, 2020, 5:49 AM EDT Project Member

Status: Assigned (was: WontFix)

adetaylor@: Please reopen if you think extra security assessment is needed beyond the analysis in #c3.

Comment 6 by guidou@chromium.org on Thu, May 21, 2020, 5:50 AM EDT Project Member

Status: WontFix (was: Assigned)

Comment 7 by a_deleted_user on Thu, May 21, 2020, 8:43 PM EDT

Btw this is now being discussed here: https://bugs.chromium.org/p/webrtc/issues/detail?id=11597#c1

Proposed patch is here: https://webrtc-review.googlesource.com/c/src/+/175960

Comment 8 by kenrb@chromium.org on Mon, May 25, 2020, 3:33 PM EDT Project Member

Status: ExternalDependency (was: WontFix)
Labels: Security_Impact-Stable Security_Severity-Low M-85 OS-Android OS-Chrome OS-Linux OS-Mac OS-Windows Pri-2

Responding to #c3: I think the additional privacy exposure is that the DNS server is exposed to a WebRTC peer rather than a website that the victim is visiting. Since a fix is in progress this can serve as a downstream tracking bug.

Comment 9 by hta@chromium.org on Mon, Jun 22, 2020, 7:45 AM EDT Project Member

The WebRTC fix has landed in Chrome, marking issue as fixed.

Comment 10 by hta@chromium.org on Mon, Jun 22, 2020, 7:45 AM EDT Project Member

Status: Fixed (was: ExternalDependency)

Comment 11 by natashapabrai@google.com on Mon, Jun 22, 2020, 2:05 PM EDT Project Member

Labels: reward-topanel

Comment 12 by sheriffbot on Mon, Jun 22, 2020, 3:06 PM EDT Project Member

Labels: -Restrict-View-SecurityTeam Restrict-View-SecurityNotify

Comment 13 by natashapabrai@google.com on Wed, Jun 24, 2020, 7:22 PM EDT Project Member

Labels: -reward-topanel reward-0

Unfortunately the Panel declined to award this report.

Comment 14 by adetaylor@google.com on Mon, Jul 13, 2020, 1:34 PM EDT Project Member

Note to self: Commit 743b9b258c4eda14ce0e13ee80873fcd3ca2aafb from #c7 landed in M85 branch.

Comment 15 by adetaylor@google.com on Thu, Aug 20, 2020, 2:22 PM EDT Project Member

Labels: Release-0-M85

Comment 16 by adetaylor@google.com on Mon, Aug 24, 2020, 3:29 PM EDT Project Member

Labels: CVE-2020-6570 CVE_description-missing

Comment 17 by adetaylor@google.com on Mon, Sep 21, 2020, 3:05 PM EDT Project Member

Labels: -CVE_description-missing CVE_description-submitted

Comment 18 by sheriffbot on Mon, Sep 28, 2020, 3:03 PM EDT Project Member

Labels: -Restrict-View-SecurityNotify allpublic

This bug has been closed for more than 14 weeks. Removing security view restrictions.

For more details visit https://www.chromium.org/issue-tracking/autotriage - Your friendly Sheriffbot