# عنوان مستند

# نقص در کد سمت کلاینت سایتها در مرورگرChrome موجب جاسوسی صوتی و تصویری از کاربران می‌شوند

فهرست مطالب

# ۱ چکیده

چه اتفاقی می افتد اگر لپتاپ شما بدون اطلاعتان ویدیویی از محیط اطراف شما ضبط کند یا صدای شما را در حین مکالمه تلفنی یا صحبت کردن با کسی ضبط کند؟ این سناریو نه تنها ترسناک به نظر می رسد بلکه انجام شدنی نیز می باشد.

یک نقض طراحی UX در مرورگر Chrome اجازه می دهد وب سایت های مخرب صدا یا ویدئو کاربر را بدون هیچگونه هشدار یا نشانه های بصری ضبط کنند و بدین صورت کاربر مورد سوء استفاده قرار گیرد.

این آسیب پذیری در دهم اپریل ۲۰۱۷ توسط یک توسعه‌دهنده AOL به گوگل گزارش شد اما این غول فناوری این آسیب پذیری را بعنوان یک مسئله امنیتی معتبر نپذیرفت که به معنی این است که هیچ وصله امنیتی رسمی برای این آسیب پذیری در کار نیست.

# ۲ محصولات تحت تاثیر

این آسیب‌پذیری ورژن ۵۷.۰.۲۹۸۷ مرورگر Google chrome و سیستم‌عامل ویندوز ۱۰، ۶۴ بیتی ورژن ۱۶۰۷ و ساخته ۱۴۳۹۳.۹۵۳ را تحت تاثیر قرار می‌دهد

# ۳ پروتکل WebRTC

قبل از پرداختن به جزئیات آسیب‌پذیری لازم است بدانیم که ارتباطات ویدیویی و صوتی که از طریق مرورگرها انجام می‌شوند برمبنای پروتکل WebRTC (Web Real-Time Communications) می‌باشد.

پروتکل WebRTC مجموعه ای از پروتکل های ارتباطی است که توسط اکثر مرورگرهای وب مدرن پشتیبانی می شوند تا ارتباط بلادرنگ را در ارتباطات نظیر به نظیر ( peer-to-peer ) بدون استفاده از پلاگین‌ها فعال کنند.

با این وجود برای جلوگیری از پخش غیرمجاز صوتی و تصویری بدون اجازه کاربر، ابتدا مرورگر از کاربران درخواست می‌کند که با صراحت اجازه‌ی استفاده وب‌سایت از پروتکل WebRTC و دسترسی به دوربین و میکروفن دستگاه را بدهد. با این فرض وب‌سایت برای همیشه به دوربین و میکروفن دستگاه ما دسترسی خواهد داشت تا زمانی که ما به صورت دستی امتیاز پروتکل WebRTC را باطل کنیم.

در گوگل کروم نیز یک آیکن به شکل نقطه قرمز ظاهر می‌شود که کاربران در مورد جریان ضبط زنده صوتی و تصویری اطلاع می‌دهد.

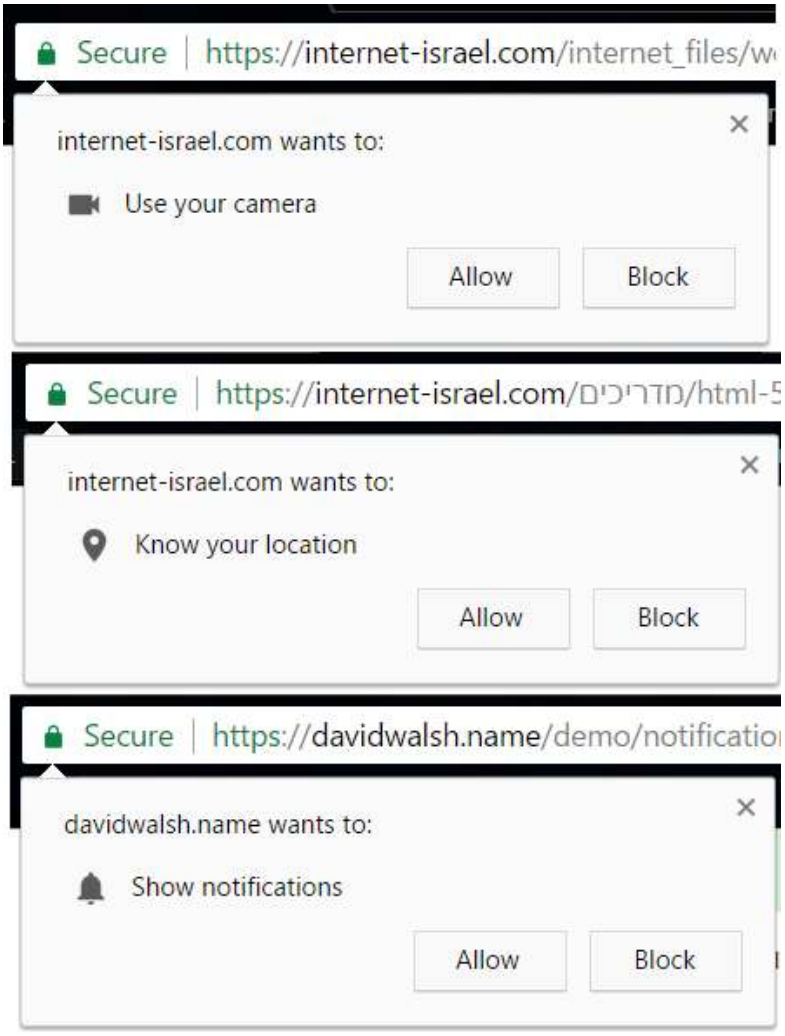
# ۴ جزییات آسیب‌پذیری

API جدید HMTL۵ اجازه گرفتن خروجی صوتی و تصویری را از مرورگر می‌دهد. برای اینکار نیازی به استفاده از واسطه‌های سخت و محلی ویندوز یا پلاگین‌های عجیب مرورگر نمی‌باشد. هر دو مرورگر فایرفاکس و کروم (و مرورگر Edge نیز به زودی) اجازه دسترسی به دوربین لپ‌تاپ، تبلت،گوشی یا هر وسیله دیگر را می‌دهند که این کار فوق العاده است، زیرا برخی از برنامه های کاربردی مانند Google Hangouts و بسیاری از سایت های ویدئو چت دیگر را فعل می سازد. اما همچنان دارای برخی خطرات امنیتی است. برای مقابله با این خطرات، توسعه دهندگان مرورگرها دو مانع را ایجاد کرده اند که باعث جلوگیری یا حداقل کاهش نقض حریم خصوصی شوند.

```
const constraints = {
  audio: true,
  video: true
};
navigator.mediaDevices.getUserMedia(constraints).
then((stream) => {
  handleSuccess(stream); // This is basic handler with stream input.
});
```

**شکل (۱)**

کد موجود در شکل (۱) کد پایه جاوا اسکریپت برای شروع دسترسی به دستگاه های صوتی و تصویری است. اجرای این کد باعث می شود که مرورگر از کاربر درخواست اجازه استفاده عمومی از دستگاه های صوتی و تصویری را بدهد. در مرورگر Chrome، این درخواست اجازه دسترسی به دستگاه های صوتی و تصویری همانند درخواستهای دیگر است.




**شکل (۲ ) انواع مختلف درخواست‌های اجازه دسترسی در مرورگر Chrome**

ممکن است بسیاری از کاربران، شاید حتی شما، یکی از این درخواست های شکل(۲) را تایید کنند. از آنجایی که بسیاری از سایت های خبری درخواست اطلاع رسانی می کنند و بسیاری از سایت های رستوران ها، هتل ها و مراکز خدماتی درخواست فهمیدن محل را می کنند، کاربران فقط این درخواست ها را تأیید می کنند و در مورد آن خیلی فکر نمی کنند.

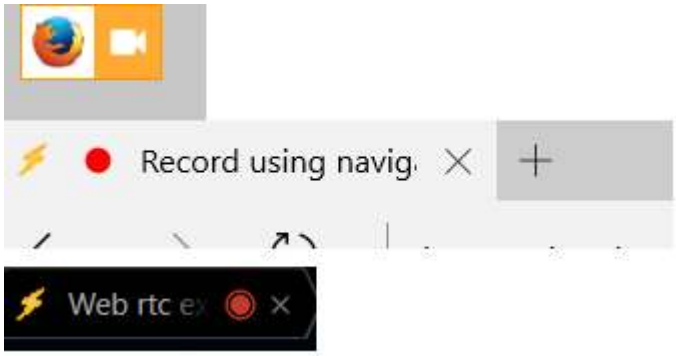
اما جای ترس نیست، زیرا یک خط دفاعی مهم دیگری نیز وجود دارد. بعد از گرفتن اجازه عمومی کاربر برای استفاده صوتی و تصویری، توسعه دهنده به جریانی از اطلاعات از طریق دستگاه‌های صوتی و تصویری دسترسی پیدا می‌کند، اما برا استفاده از این جریان اطلاعاتی توسعه‌دهنده باید آن را ضبط کند. این کار با استفاده از MediaRecorder API انجام می شود.

```
const recordedBlobs = [];
const mediaRecorder = new window.MediaRecorder(window.stream,{
mimeType: 'audio/mpeg' });
mediaRecorder.ondataavailable = (event) => {
  recordedBlobs.push(event.data);
};

mediaRecorder.start();
```

**شکل (۳)**

فعالسازی این API به کاربر هشدار می‌دهد که یکی از دستگاه‌های صوتی و تصویری در حال ضبط صدا و تصویر می‌باشد. مرورگرهای Chrome و Firefox این هشدار را پیاده‌سازی کرده‌اند ( این قابلیت در مرورگر Edge هنوز موجود نیست. ).




**شکل (۴) علامت ضبط در مرورگر های Chrome و Firefox**

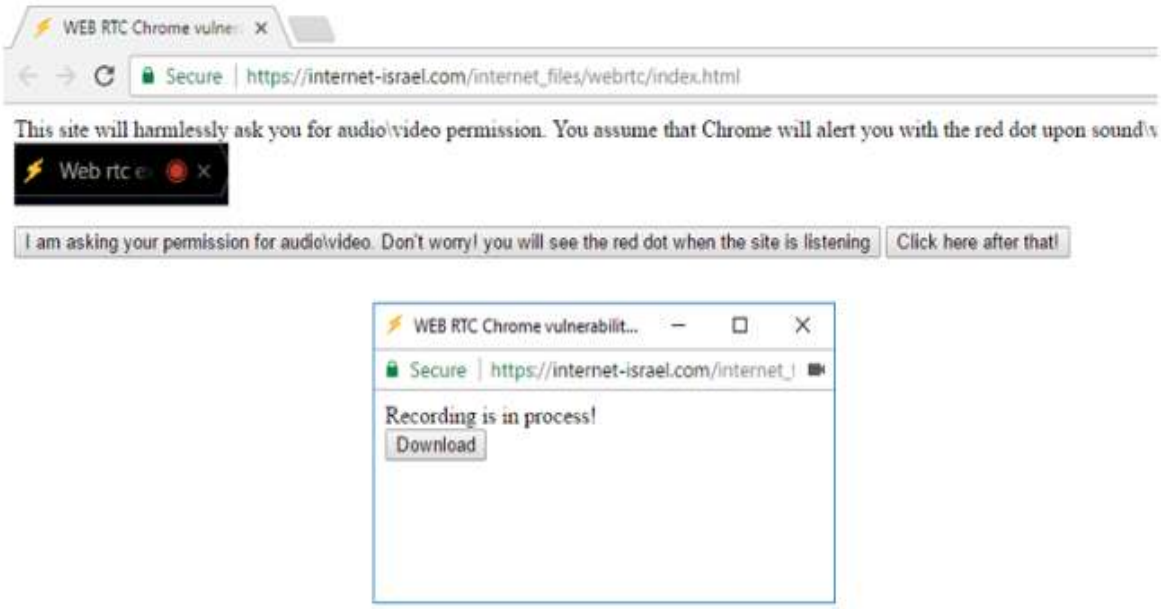
این علامت رکورد در شکل (۴) اخرین و مهمترین خط دفاعی می‌باشد. اجازه کلی استفاده از دستگاه صوتی و تصویری فقط یکبار از کاربر درخواست می‌شود که کاربر ممکن است خطا کند و آن را بپذیرد. آخرین خط دفاعی زمانی است که این درخواست پذیرفته شود. هشدار ضبط در هر مورد استفاده از جریان رکورد داده می‌شود و بدون اطلاع کاربر از هر ضبطی ممانعت می‌کند.

## ۴-۱ قابلیت بهره برداری

اما روال کار همیشه اینگونه نمی‌باشد بطوریکه توسعه دهندگان می توانند از یک نقض که با دستکاری کوچک در UX به وجود می‌آید برای فعال کردن MediaRecorder API بدون هشدار دادن به کاربران بهره برداری کنند.

این فرایند کاملا ساده است. به این صورت که بعد از اعطای دسترسی عمومی توسط کاربر یک پنجره باز میشود که از آن پنجره MediaRecorder فعال می‌شود. در Chrome هیچ نشانه ای از ضبط بصری وجود نخواهد داشت.

برای این آسیب‌پذیری یک صفحه دموی کوچک پیاده‌سازی شده است که دو دکمه دارد. دکمه اول فقط اجازه دستگاه را درخواست می‌کند. بسیاری از سایت‌ها این درخواست را می‌کنند و اکثر کاربران بدون هیچگونه فکری این درخواست را می‌پذیرند. دکمه دوم حمله را شبیه‌سازی می‌کند که فرایند آن آسان می‌باشد به اینصورت که یک پنجره بدون سربرگ باز می‌شود و شروع به ضبط از کاربر می‌کند. تمام کاری که باید در این صفحه دمو انجام شود این است که روی این دکمه کلیک شود تا به وب‌سایت‌ها اجازه استفاده از پروتکل WebRTC در مرورگر داده شود. بعد ۳۰ ثانیه شما می‌توانید تصویر یا صدای ضبط شده را بصورت MP۳ از کامپیوتر دانلود کنید.



شکل(۵)

لینک ذیل مربوط به صفحه دمو مذکور می‌باشد:

https://internet-israel.com/internet_files/webrtc/index.html

البته حمله واقعی کاملا مشخص نیست. این حمله از صفحات pop-under بسیار کوچک استفاده می‌کند و هنگامی‌که کاربر روی صفحه pop-under متمرکز می‌شود آن را می‌بندد. صفحات pop-under برعکس صفحات pop-up در یک سربرگ (tab) جداگانه باز می‌شوند و زیر صفحه اصلی نمایش داده می‌شوند، بنابراین کاربر به‌سختی متوجه ظاهر شدن آنها می‌شود. درواقع pop-under ها صفحاتی هستند که زیر صفحه اصلی نمایش داده می‌شوند. این حمله برای چند میلی ثانیه از دوربین برای گرفتن عکس استفاده می‌کند. این حمله می‌تواند از XSS برای سوار شدن بر روی سایت‌های مجاز و مجوزهایشان استفاده کند.

در موبایل چنین نشانه بصری وجود ندارد، اما به کاربران بیشتر در مورد مجوز مرورگرها هشدار داده می‌شود.

# ۵ اقدامات جهت کاهش شدت آسیب پذیری

این آسیب‌پذیری به گوگل گزارش شده است اما این شرکت آسیب‌پذیری مذکور را به عنوان یک مسئله امنیتی معتبر نپذیرفت که به معنی این است که هیچ وصله امنیتی رسمی برای این آسیب پذیری در کار نیست. اما گوگل اعلام کرده است که در آینده راهکاری برای بهبود این شرایط پیدا خواهد کرد.

به منظور حفظ امنیت، به راحتی می‌توان پروتکل WebRTC را غیرفعال کرد که اگر به آن نیازی نباشد می‌توان به راحتی انجام داد. اما اگر به این ویژگی نیاز باشد، وبسایت‌های معتبر را مجاز به استفاده از پروتکل WebRTC کنید و مراقب هر پنجره دیگری که ممکن است پس از آن در بالای صفحه ظاهر شود، باشید.

هرچند که گذاشتن نوار بر روی وب‌کم نمی‌تواند مانع از رکورد صدای کاربر توسط هکرها و آژانس‌های جاسوسی دولت شود اما حداقل می‌تواند مانع از گرفتن عکس یا ضبط ویدیوی شما شود.

# ۶ جمع بندی و نتیجه‌گیری

API جدید صوتی وتصویری HMTL۵ دارای مسائل مربوط به حریم خصوصی در نسخه دسکتاپ مرورگر کروم می‌باشد.

اگر در هر وب‌سایت مجازی یک پنجره بدون سربرگ بی سرو صدا ایجاد شود که از کدهای جاوا اسکریپت استفاده می‌کند، می تواند شروع به ضبط مخفیانه صدا و تصویر کند که این اتفاق بدون هیچگونه آیکن نقطه قرمز یا دادن هرگونه نشانه در مرورگر اتفاق می‌افتد.

برای این آسیب‌پذیری که باعث جاسوسی از کاربران می‌شود به زودی وصله امنیتی از طرف گوگل منتشر نخواهد شد.

# ۷ منابع

[۱] https://medium.com/@barzik/the-new-html۵-video-audio-api-has-privacy-issues-on-desktop-chrome-۵۸۳۲c۹۹c۷۶۵۹

[۲] http://thehackernews.com/۲۰۱۷/۰۵/browser-camera-microphone.html?m=۱