هشدار آسیب‌پذیری			
موضوع	کشف و شناسایی یک آسیب‌پذیری روز صفرم جدید بر روی کروم		
شماره هشدار	۲۲	**تاریخ صدور هشدار**	۱۱ آبان ۱۳۹۸
تشریح تهدید	با انتشار مرورگر کروم نسخه ۷۸.۰.۳۹۰۴.۸۷، گوگل به کاربران خود هشدار داده است که به سرعت یک به‌روزرسانی اورژانسی برای رفع دو آسیب‌پذیری را نصب کنند. یکی از این آسیب‌پذیری‌ها به سرعت در حال بهره‌برداری توسط مهاجمین است. تیم امینتی کروم بدون اینکه جزئیاتی زیادی درباره این دو آسیب‌پذیری انتشار دهد، گفته است که هر دو آسیب‌پذیری مذکور از نوع آسیب‌پذیری استفاده پس از آزادسازی (use-after-free) هستند که مولفه صوت کروم (با شناسه CVE-2019-13720) و کتابخانه PDFium (با شناسه CVE-2019-13721) را تحت تاثیر قرار می‌دهند. پژوهشگران کسپرسکی با نام Anton Ivanov و Alexey Kulaev کشف و شناسایی کرده‌اند که به صورت فعالانه مهاجمین در حال بهره‌برداری از این آسیب‌پذیری‌ها هستند. به هر صورت، آسیب‌پذیری استفاده پس از آزادسازی یکی از رایج‌ترین آسیب‌پذیریهایی است که در ماه اخیر در مرورگر کروم کشف و شناسایی شده است. در هر صورت، این دو آسیب‌پذیری به یک مهاجم اجازه خواهند سطح دسترسی بر روی مرورگر کروم به دست آورند و همچنین در ادامه محافظت‌های سندباکس کروم را دور بزنند و همچنین در ادامه کد دلخواه بر روی سامانه آسیب‌پذیر اجرا کنند.		
راه‌حل کاهش تهدید	این آسیب‌پذیری‌ها تمامی نسخه‌های مرورگر کروم را تحت تاثیر قرار می‌دهند. برای رفع آسیب‌پذیری‌های مذکور کافی است مرورگر کروم را به آخرین نسخه و همچنین آخرین وصله‌های امنیتی به‌روزرسانی کنید.		
شناسه آسیب‌پذیری	CVE-2019-13721 CVE-2019-13720	**شدت آسیب‌پذیری**	High High
منابع	https://chromereleases.googleblog.com/2019/10/stable-channel-update-for-desktop_31.html		