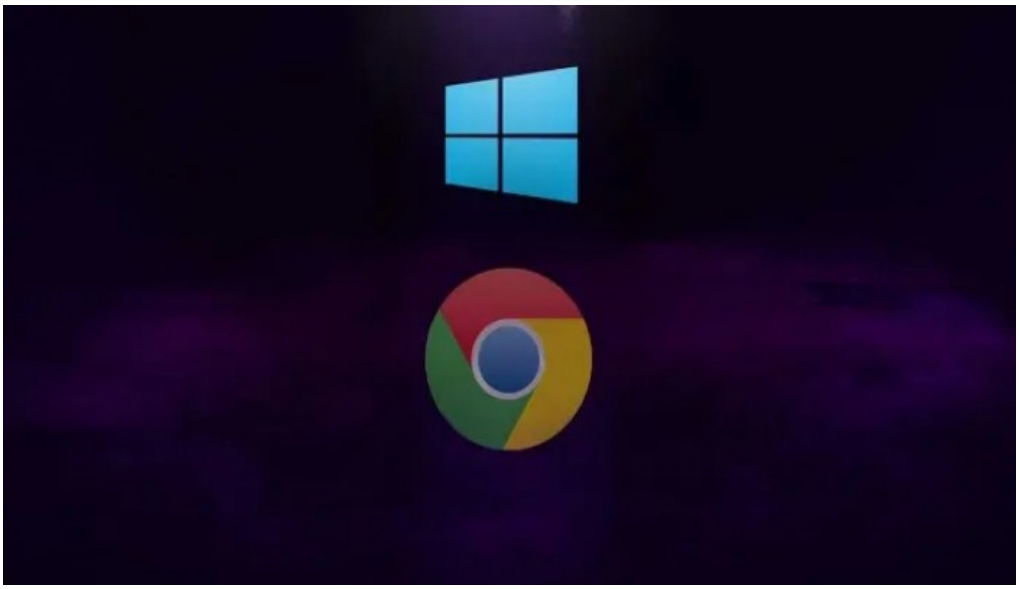
جوجل تكشف عن ثغرة في ويندوز وهي مُستغلّة الآن



السبت 31 أكتوبر 2020 11:10 م

كشف فريق (بروجكت زيرو) Project Zero التابع لشركة جوجل والمعروف باكتشافه تهديدات أمنية عن ثغرة أمنية في نظام ويندوز ، والتي توثر على الإصدارات من (ويندوز 7)، وحتى الإصدار 1903 من نظام (ويندوز 10).

وقالت جوجل في منشور: إنه لديها دليل على عمليات استغلال نشطة للثغرة الأمنية المتكشفة، والتي تسمح للمهاجمين بتنفيذ تعليمات برمجية بأذونات متقدمة

والأمر المثير للاهتمام هو أن الثغرة الأمنية التي يجري تتبعها باستخدام التسمية CVE-2020-17087، إلى جانب ثغرة أخرى استُغلّت بنشاط في متصفح كروم وقد كُشف عنها الأسبوع الماضي CVE-2020-15999، تؤدي ما يُعرف باسم الهروب من وضع الحماية، حيث يستفيد فيه المجرم الإلكتروني من هاتين الثغرتين لتنفيذ التعليمات البرمجية في هدف مخترق عن طريق الهروب من البيئة الآمنة للمتصفح، وذلك وفق ما أوضح (كاتالين سيمبانو) من موقع ZDNet التقني

ويضيف منشور الكشف أيضًا أن مايكروسوفت ستصلح هذه الثغرة الأمنية من خلال تحديثات Tuesday Patch القادم في 10 تشرين الثاني/ نوفمبر ومع ذلك، فإن إصلاحات إصدارات ويندوز 7 ستجعلها فقط للمستخدمين الذين اشتركوا في تحديثات الأمان الموسعة ESU لذلك لن يتمكن جميع المستخدمين من إصلاح المشكلة في أنظمة ويندوز 7 الخاصة بهم ونظرًا لاستغلال الثغرة على نحو نشط، قدم فريق عملاق البحث لشركة مايكروسوفت سبعة أيام لتصحيح الخطأ قبل الكشف عنه علنًا اليوم

وقامت جوجل بالفعل بتصحيح الثغرة الأمنية في متصفح كروم بإصدار النسخة المستقرة 86.0.4240.1111 من المتصفح وبالنسبة إلى ثغرة ويندوز، تكمن الثغرة الأمنية في برنامج تشغيل تشفير (cng.sys Windows Kernel)، والذي يشرحه فريق Project Zero بالتفصيل في المنشور وقامت الشركة أيضًا بإرفاق رمز إثبات المفهوم لإظهار كيف يمكن أن يؤدي الاستغلال إلى تعطل النظام

وبالإضافة إلى ذلك، أكد (شين هانتلي) – المدير الخاص بمجموعة تحليل التهديدات في جوجل أن الثغرة لا تتعلق بأي هجوم ترعاه الحكومات على الانتخابات الأمريكية المقبلة