الخليج

اقتصاد, تقنية وسيارات

12 مايو 2022 16:55 مساء

«مجرمو الإنترنت ينشطون لاستغلال ثغرات بنظام «ويندوز



دبي: «الخليج»

ضمن نظام Print Spooler كشف باحثو كاسبرسكي عن أن عدد الهجمات التي تستغل الثغرات الموجودة في برمجية التشغيل ويندوز, قد شهد ارتفاعًا ملحوظًا خلال الأشهر الأربعة الماضية. ويواصل مجرمو الإنترنت استغلال تلك الثغرات بنشاط، بالرغم من أن مايكروسوفت تصدر بانتظام تصحيحات لهذه البرمجية التي تدير عملية الطباعة. ويتيح الفرصة للمجرمين لتوزيع البرمجيات الخبيثة وتثبيتها على أجهزة Print Spooler استغلال الثغرات الموجودة في الحاسوب المستهدفة لسرقة البيانات المخزنة عليها.

لنظام التشغيل ويندوز، والتي استغلها Print Spooler واكتُشفت خلال العام الماضي العديد من الثغرات الأمنية في مجرمو الإنترنت للسيطرة على الخوادم والأجهزة، من دون الحاجة إلى إذن وصول الخاص بالمسؤول التقني.

من أشهر (PrintNightmare المعروفة أيضًا بالاسم) CVE-2021-34527وCVE-2021-1675 وتُعتبر الثغرتان من دون قصد باعتبارها مثالًا PrintNightmare الثغرات، وكانتا اكتُشفتا في أواخر يونيو 2021. وقد نُشرت الثغرة لتطوير GitHub وبالرغم من أن الثغرة سرعان ما أزيلت من منصة .Print Spooler على استغلال ثغرة في البرمجيات، التابعة لمايكروسوفت، فقد تمكّن بعض المستخدمين من تنزيلها ثم أعادوا نشرها. واكتُشفت ثغرة خطرة

وأصدرت Print Spooler في (CVE-2022-22718 أخرى في أواخر إبريل 2022 (جرى تعقبها بالرمز مايكروسوفت تصحيحًا لها، لكن المهاجمين ظلوا قادرين على استغلالها والوصول إلى الموارد المؤسسية من خلالها. واكتشف باحثو كاسبرسكي أن مجرمي الإنترنت نفذوا ما يقرب من 65,000 هجوم باستغلال هذه الثغرات بين يوليو 2021 وإبريل 2022، ووجدوا أن ما يقرب من 31,000 من هذه الهجمات حدثت خلال الأشهر الأربعة الماضية؛ بين طريق شائع الاستخدام في شنّ الهجمات، Print Spooler يناير وإبريل. وتشير هذه الأرقام إلى أن الثغرات الأمنية في ما يشدّد على أهمية حرص المستخدمين على متابعة التصحيحات وتثبيتها حال صدورها من مايكروسوفت.

العديد من البلدان؛ فحدث ما يقرب من Print Spooler وضربت الهجمات المتزايدة التي تستغل الثغرات الأمنية في ربع الحالات المكتشفة بين يوليو 2021 وإبريل 2022 في إيطاليا، التي تلتها في عدد الهجمات تركيا فكوريا الجنوبية. ووجد باحثو كاسبرسكي أيضًا أن المهاجمين كانوا أنشط في النمسا وفرنسا وسلوفينيا في الأشهر الأربعة الماضية.

معبر نشط» Print Spooler واعتبر أليكسي كولايف الباحث الأمني لدى كاسبرسكي، أن الثغرات الموجودة في للتهديدات الجديدة الناشئة»، مرجّحًا تزايد محاولات استغلال هذه الثغرات للوصول إلى الموارد المؤسسية وتعريضها لأخطار عالية تتمثل ببرمجيات الفدية وسرقة البيانات. وقال: «بوسع المهاجمين أن يصلوا حتى إلى خوادم الشركات من خلال بعض هذه الثغرات، ولذلك نوصي بشدّة بأن يتبع المستخدمون إرشادات مايكروسوفت وأن يطبقوا أحدث .«التحديثات الأمنية الخاصة بالنظام التشغيل ويندوز

"حقوق النشر محفوظة "لصحيفة الخليج .2024 ©